Experiment No. 7

Aim: Study the use of network reconnaissance tools and apply the following: WHOIS, dig, traceroute, nslookup

Theory:

Reconnaissance (or simply Recon) is the initial phase in the Pen Testing process. The goal of recon is to gather as much information about the target as you can. More the information, the more beneficial it will be for further phases of pen testing. Most new learners underestimate this phase and ignore it but recon is the most important phase of pen testing. Your point of view for the digital world changes if you completely understand this process. Learning to successfully conduct the recon process is a valuable skill for anyone. There are two strategies of recon i.e., Active and Passive reconnaissance.

- Active Recon**:** It means interacting directly with a target to gather information. This is not recommended because it violates the rule of "hiding traces" in pen testing.
- Passive Recon**:** It means gathering information about the target using vast information present on the internet. In it, we aren't interacting directly with the target so there is no fear of recording or logging of our activity by target.

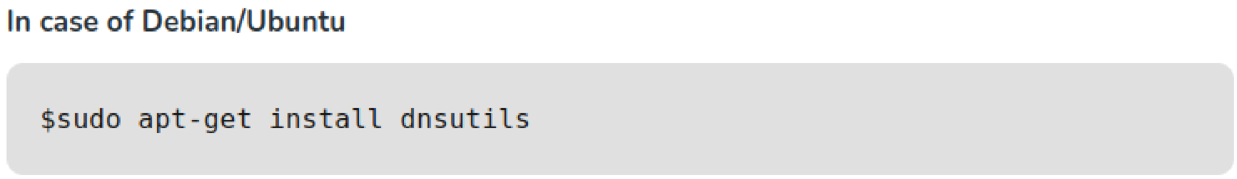
WHOIS:

Whois is a command-line utility used in Linux systems to retrieve information about domain names, IP addresses, and network devices registered with the Internet Corporation for Assigned Names and Numbers (ICANN). The data received by Whois consists of the name and contact information of the domain or IP address owner, the registration and expiration date, the domain registrar, and the server information. Whois command can be very useful for network administrators, web developers, and security professionals for achieving various tasks like checking network connectivity or troubleshooting. In this article, we will go through the usage of the Whois command on Linux (Ubuntu system).

The whois command is a useful tool for obtaining information about domain names, IP Addresses, and network devices registered with ICANN. Whois command is a simple and powerful tool that can be useful for network administration, web development, and security tasks, and every Linux user should be familiar with its usage. In this article, we have gone through the installation of the whois command and its usage in the form of examples.

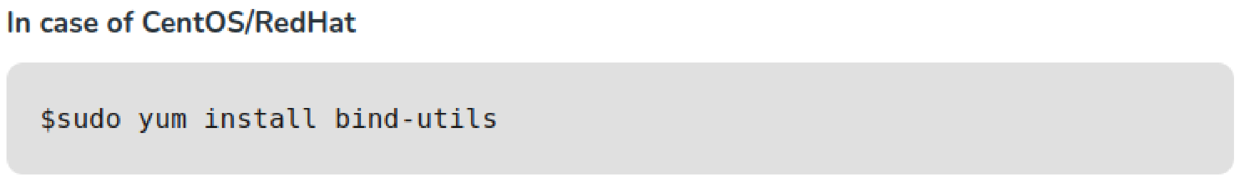
Dig:

'dig' command stands for Domain Information Groper. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.



In case of Debian/Ubuntu

```
$sudo apt-get install dnsutils
```

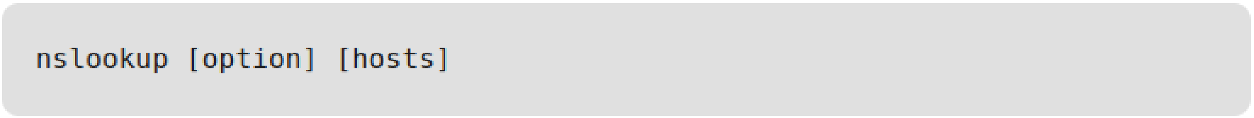


In case of CentOS/RedHat

```
$sudo yum install bind-utils
```

Nslookup:

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the 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.

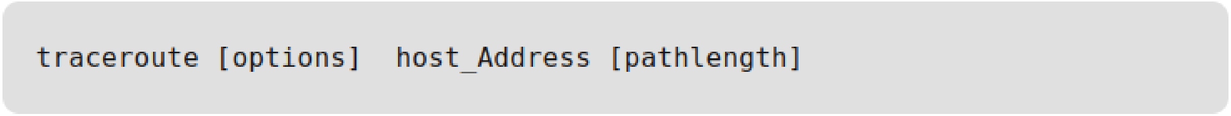


```
nslookup [option] [hosts]
```

Traceroute:

A traceroute provides a map of how data on the internet travels from its source to its destination. When you connect with a website, the data you get must travel across multiple devices and networks along the way, particularly routers.

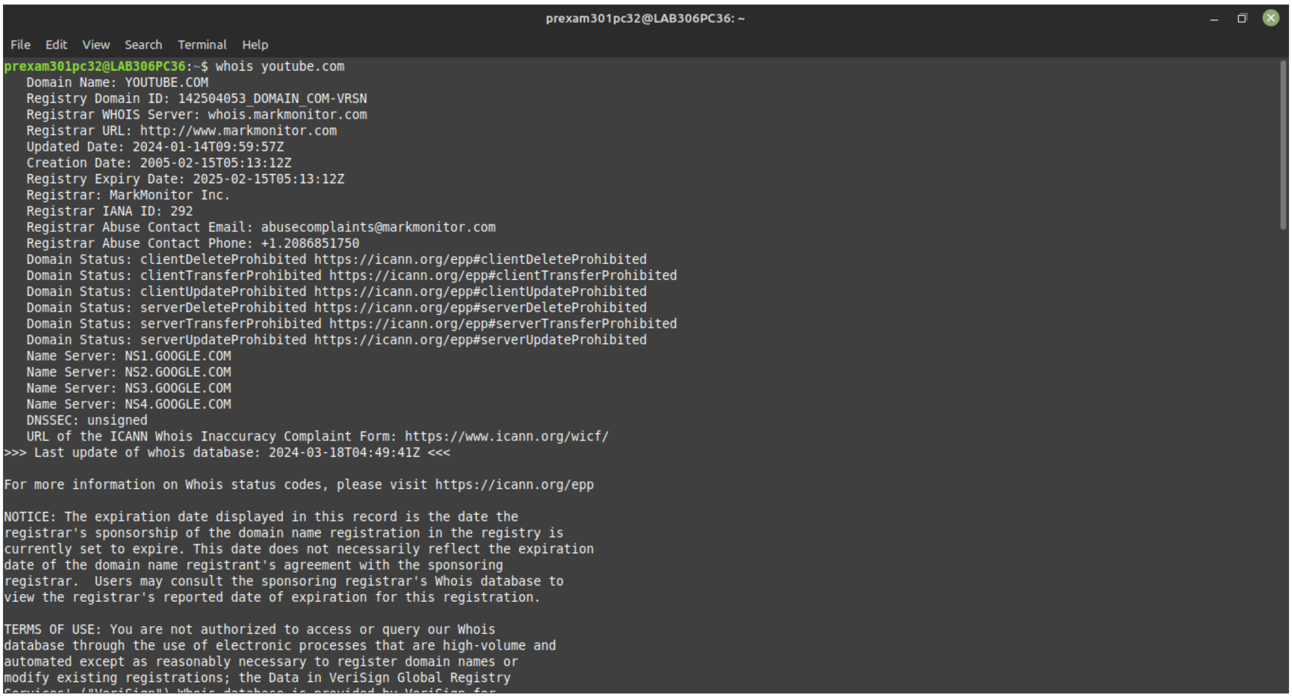
A traceroute plays a different role than other diagnostic tools, such as packet capture, which analyzes data. Traceroute differs in that it examines how the data moves through the internet. Similarly, you can use Domain Name System time to live (DNS TTL) for tracerouting, but DNS TTL addresses the time needed to cache a query and does not follow the data path between routers.



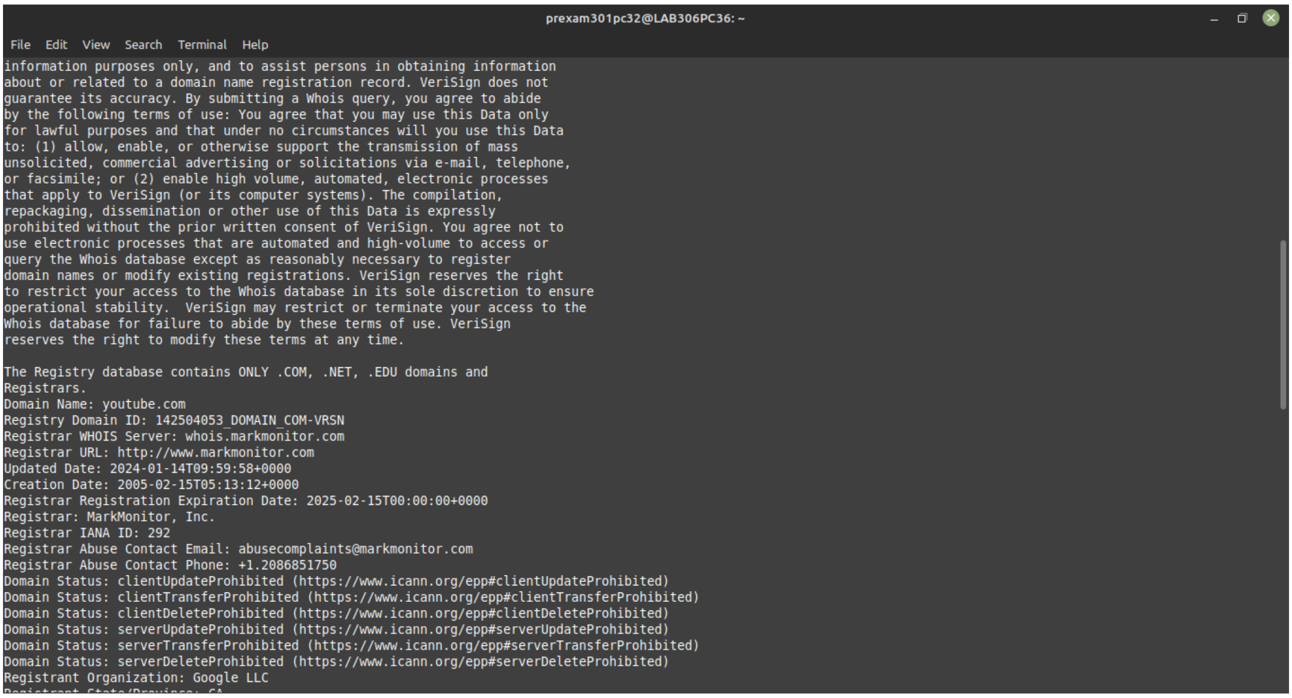
```
traceroute [options]  host_Address [pathlength]
```

Commands:

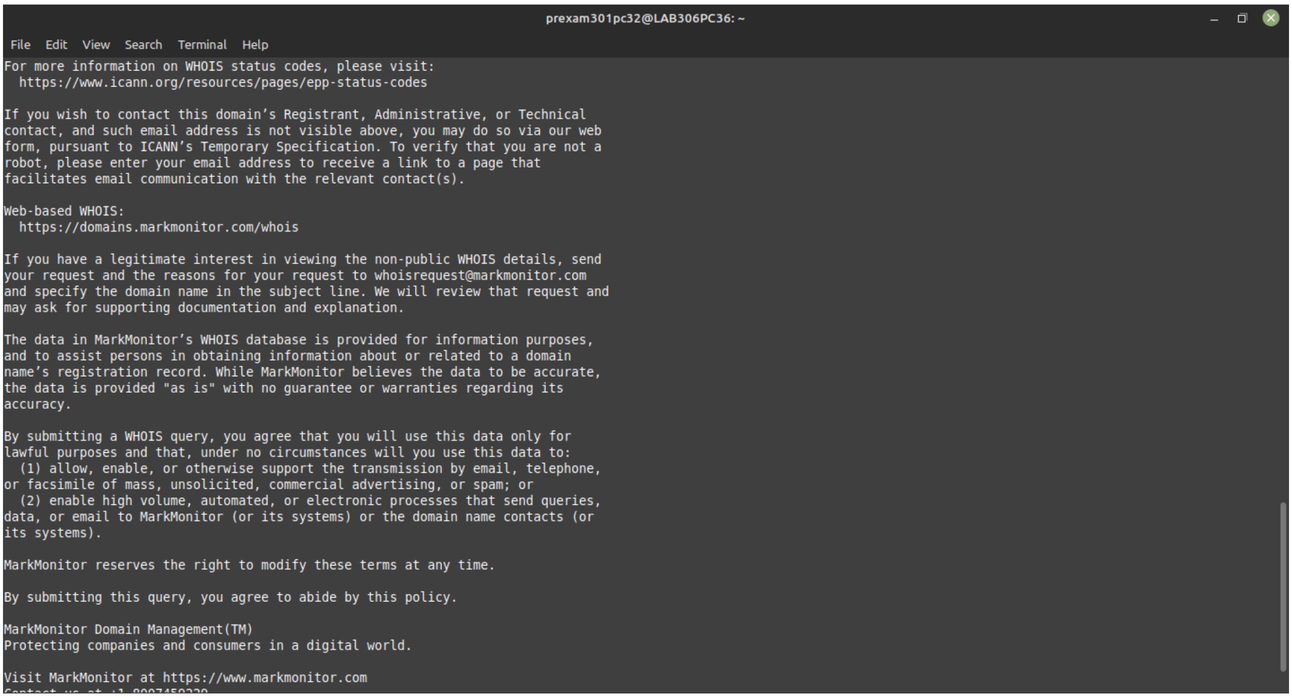
1.Whois:


prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

```
prexam301pc32@LAB306PC36:~$ whois youtube.com
   Domain Name: YOUTUBE.COM
   Registry Domain ID: 142504053_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-01-14T09:59:57Z
   Creation Date: 2005-02-15T05:13:12Z
   Registry Expiry Date: 2025-02-15T05:13:12Z
   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: 2024-03-18T04:49:41Z <<<

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
```

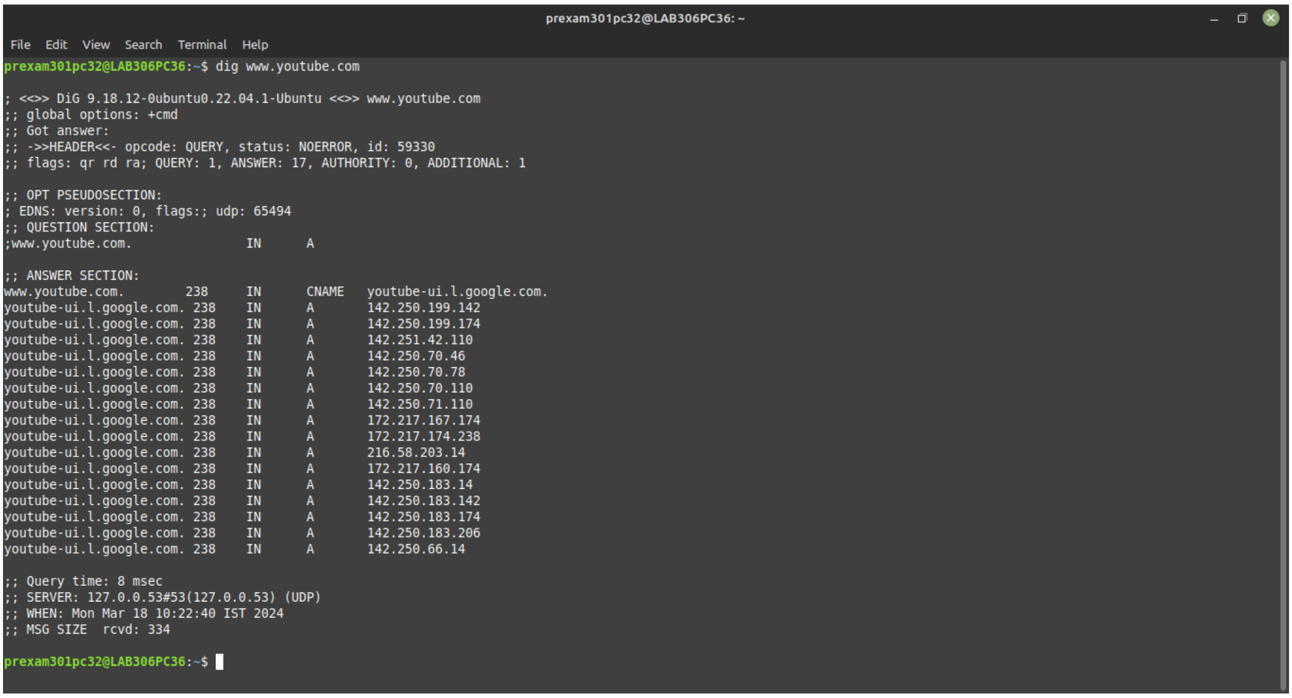

prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

```
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.
Domain Name: youtube.com
Registry Domain ID: 142504053_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2024-01-14T09:59:58+0000
Creation Date: 2005-02-15T05:13:12+0000
Registrar Registration Expiration Date: 2025-02-15T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
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
```


prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

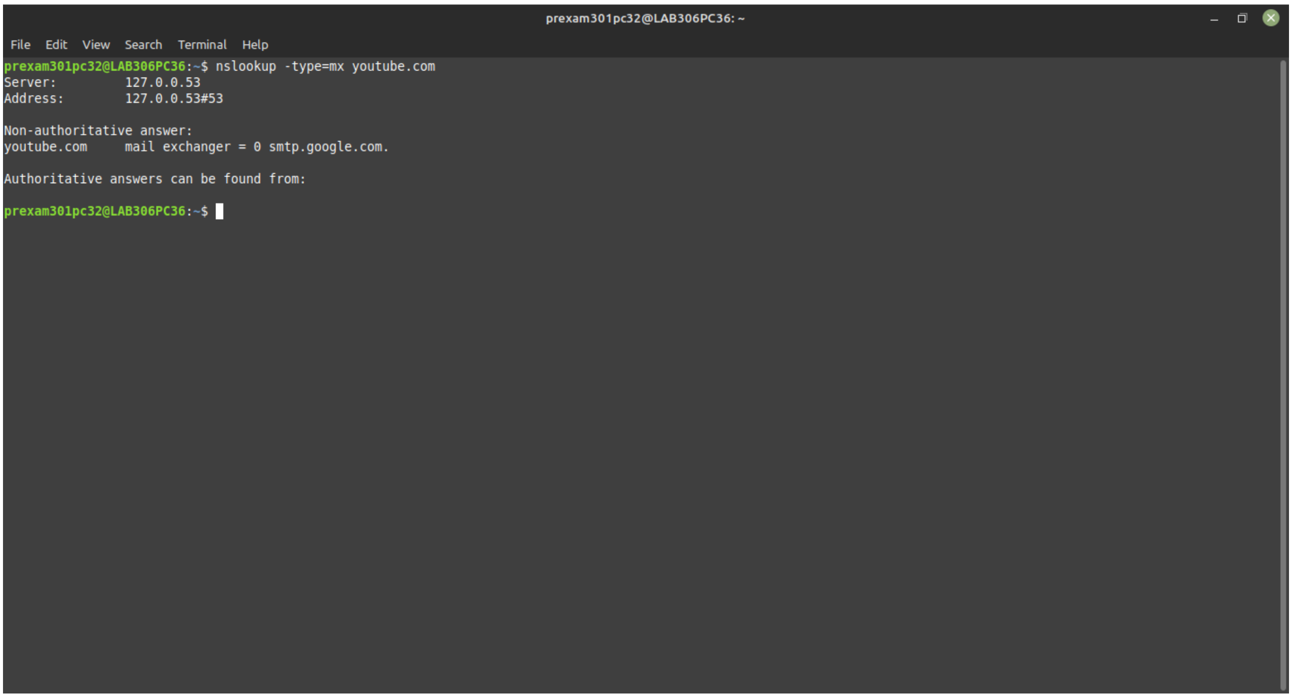
```
For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain’s Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN’s 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 MarkMonitor’s WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name’s 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
```

dig:


prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

```
prexam301pc32@LAB306PC36:~$ dig www.youtube.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.1-Ubuntu <<>> www.youtube.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59330
;; flags: qr rd ra; QUERY: 1, ANSWER: 17, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.youtube.com.               IN      A

;; ANSWER SECTION:
www.youtube.com.        238     IN      CNAME   youtube-ui.l.google.com.
youtube-ui.l.google.com. 238    IN      A       142.250.199.142
youtube-ui.l.google.com. 238    IN      A       142.250.199.174
youtube-ui.l.google.com. 238    IN      A       142.251.42.110
youtube-ui.l.google.com. 238    IN      A       142.250.70.46
youtube-ui.l.google.com. 238    IN      A       142.250.70.78
youtube-ui.l.google.com. 238    IN      A       142.250.70.110
youtube-ui.l.google.com. 238    IN      A       142.250.71.110
youtube-ui.l.google.com. 238    IN      A       172.217.167.174
youtube-ui.l.google.com. 238    IN      A       172.217.174.238
youtube-ui.l.google.com. 238    IN      A       216.58.203.14
youtube-ui.l.google.com. 238    IN      A       172.217.160.174
youtube-ui.l.google.com. 238    IN      A       142.250.183.14
youtube-ui.l.google.com. 238    IN      A       142.250.183.142
youtube-ui.l.google.com. 238    IN      A       142.250.183.174
youtube-ui.l.google.com. 238    IN      A       142.250.183.206
youtube-ui.l.google.com. 238    IN      A       142.250.66.14

;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Mar 18 10:22:40 IST 2024
;; MSG SIZE  rcvd: 334

prexam301pc32@LAB306PC36:~$ 
```

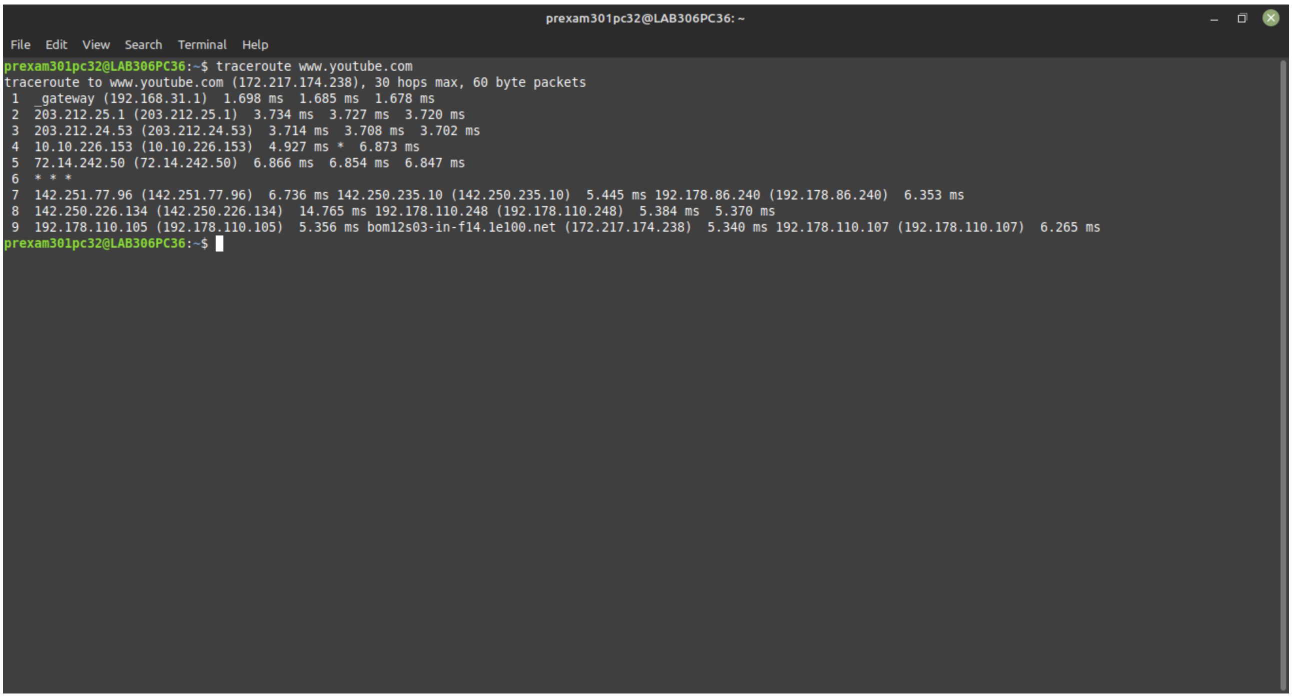
nslookup:



prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

```
prexam301pc32@LAB306PC36:~$ nslookup -type=mx youtube.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
youtube.com     mail exchanger = 0 smtp.google.com.

Authoritative answers can be found from:

prexam301pc32@LAB306PC36:~$
```

traceroute:



prexam301pc32@LAB306PC36: ~
File Edit View Search Terminal Help

```
prexam301pc32@LAB306PC36:~$ traceroute www.youtube.com
traceroute to www.youtube.com (172.217.174.238), 30 hops max, 60 byte packets
 1  _gateway (192.168.31.1)  1.698 ms  1.685 ms  1.678 ms
 2  203.212.25.1 (203.212.25.1)  3.734 ms  3.727 ms  3.720 ms
 3  203.212.24.53 (203.212.24.53)  3.714 ms  3.708 ms  3.702 ms
 4  10.10.226.153 (10.10.226.153)  4.927 ms *  6.873 ms
 5  72.14.242.50 (72.14.242.50)  6.866 ms  6.854 ms  6.847 ms
 6  * * *
 7  142.251.77.96 (142.251.77.96)  6.736 ms 142.250.235.10 (142.250.235.10)  5.445 ms 192.178.86.240 (192.178.86.240)  6.353 ms
 8  142.250.226.134 (142.250.226.134)  14.765 ms 192.178.110.248 (192.178.110.248)  5.384 ms  5.370 ms
 9  192.178.110.105 (192.178.110.105)  5.356 ms bom12s03-in-f14.1e100.net (172.217.174.238)  5.340 ms 192.178.110.107 (192.178.110.107)  6.265 ms
prexam301pc32@LAB306PC36:~$
```