# Experiment Number:6

Aim: Study the use of network reconnaissance tools like **WHOIS**, **dig**, **traceroute**, **nslookup** to gather information about networks

Date of Performance: 17-9-2020

Date of Submission: 27-9-2020

Grade:

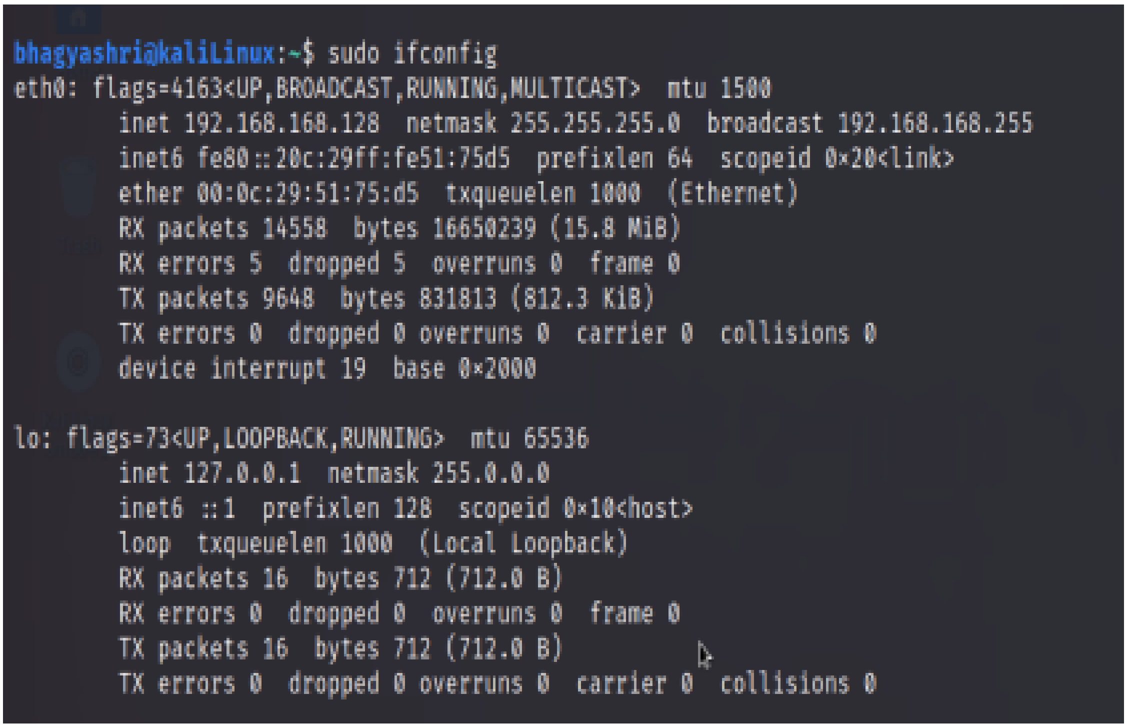
Sign:

Name : Bhagyashri Nitin Patil

Roll Number: 50

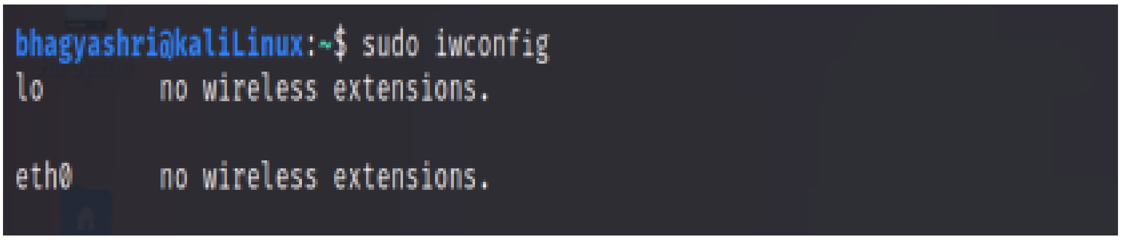
# Networking Commands

## 1. sudo ifconfig



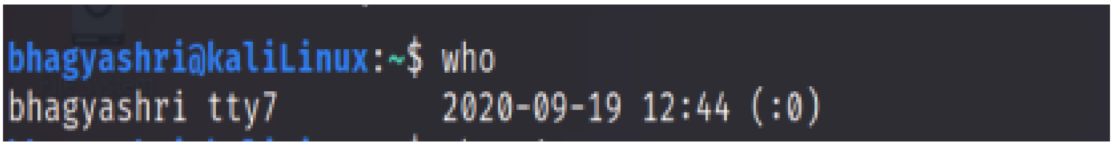
```
bhagyashri@kaliLinux:~$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.168.128  netmask 255.255.255.0  broadcast 192.168.168.255
        inet6 fe80::20c:29ff:fe51:75d5  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:51:75:d5  txqueuelen 1000  (Ethernet)
        RX packets 14558  bytes 16650239 (15.8 MiB)
        RX errors 5  dropped 5  overruns 0  frame 0
        TX packets 9648  bytes 831813 (812.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 16  bytes 712 (712.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 712 (712.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

## 2. sudo iwconfig



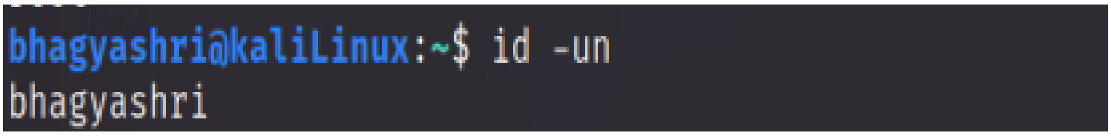
```
bhagyashri@kaliLinux:~$ sudo iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.
```

## 3. who



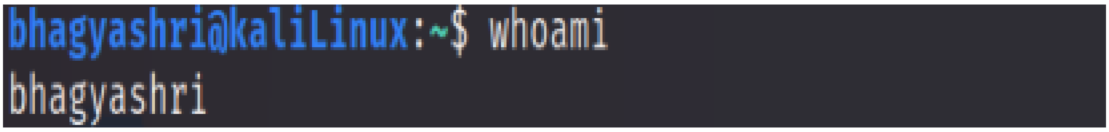
```
bhagyashri@kaliLinux:~$ who
bhagyashri tty7         2020-09-19 12:44 (:0)
```

## 4. id -un



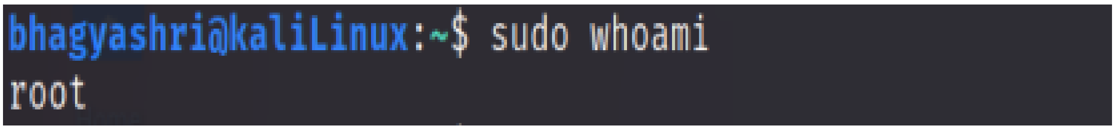
```
bhagyashri@kaliLinux:~$ id -un
bhagyashri
```

## 5. whoami



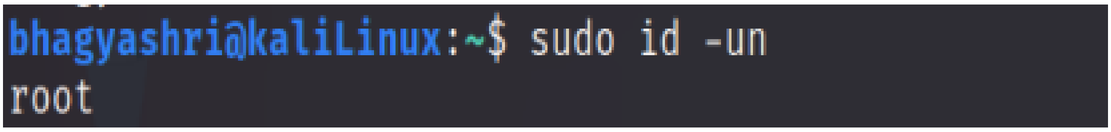
```
bhagyashri@kaliLinux:~$ whoami
bhagyashri
```

## 6. sudo whoami



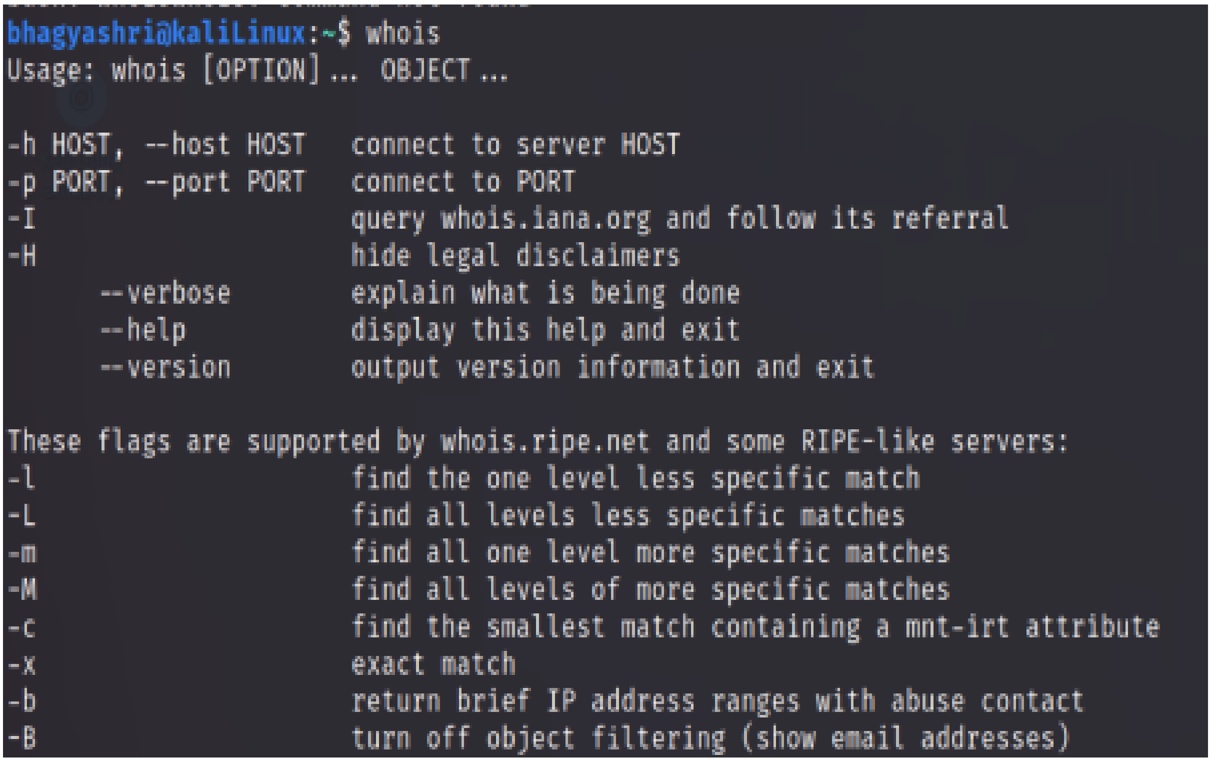
```
bhagyashri@kaliLinux:~$ sudo whoami
root
```

## 7. sudo id -un

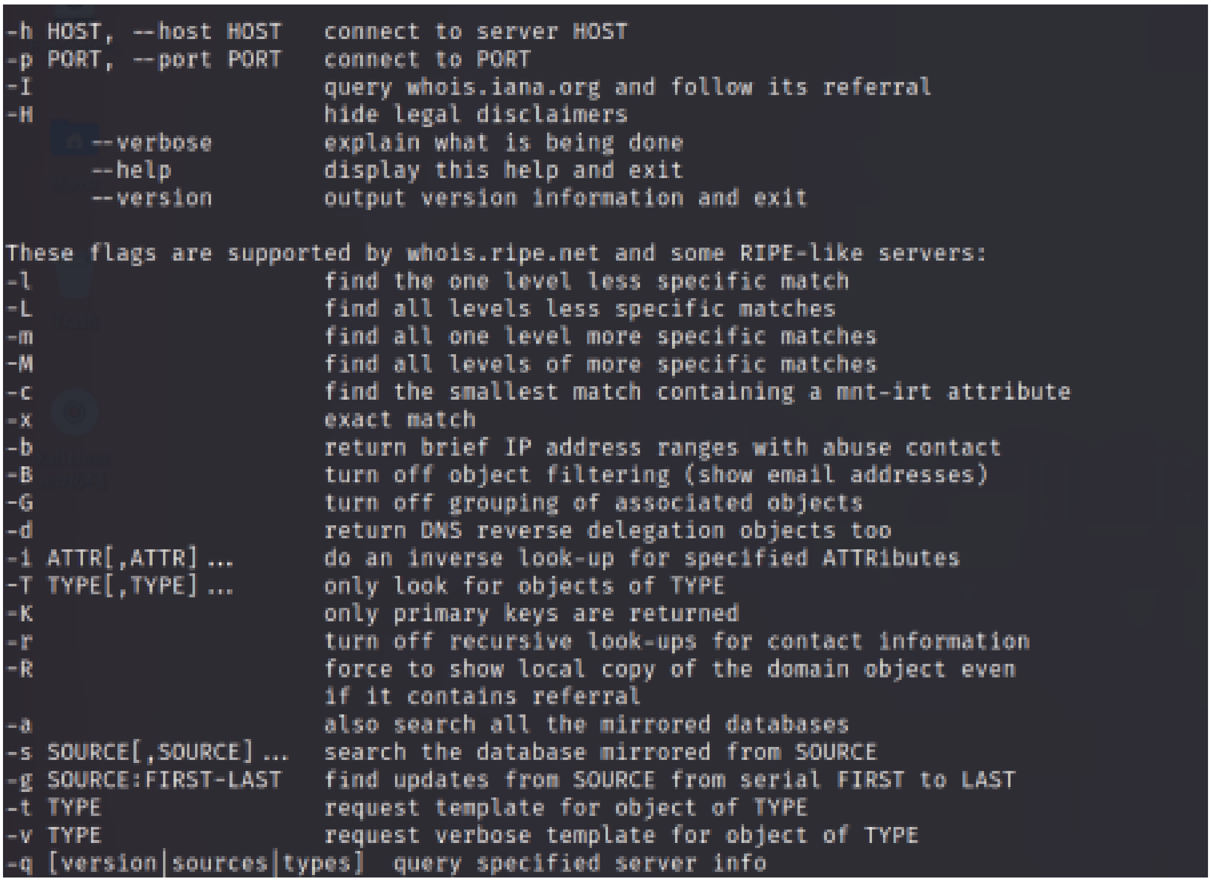


```
bhagyashri@kaliLinux:~$ sudo id -un
root
```

## 8. whois



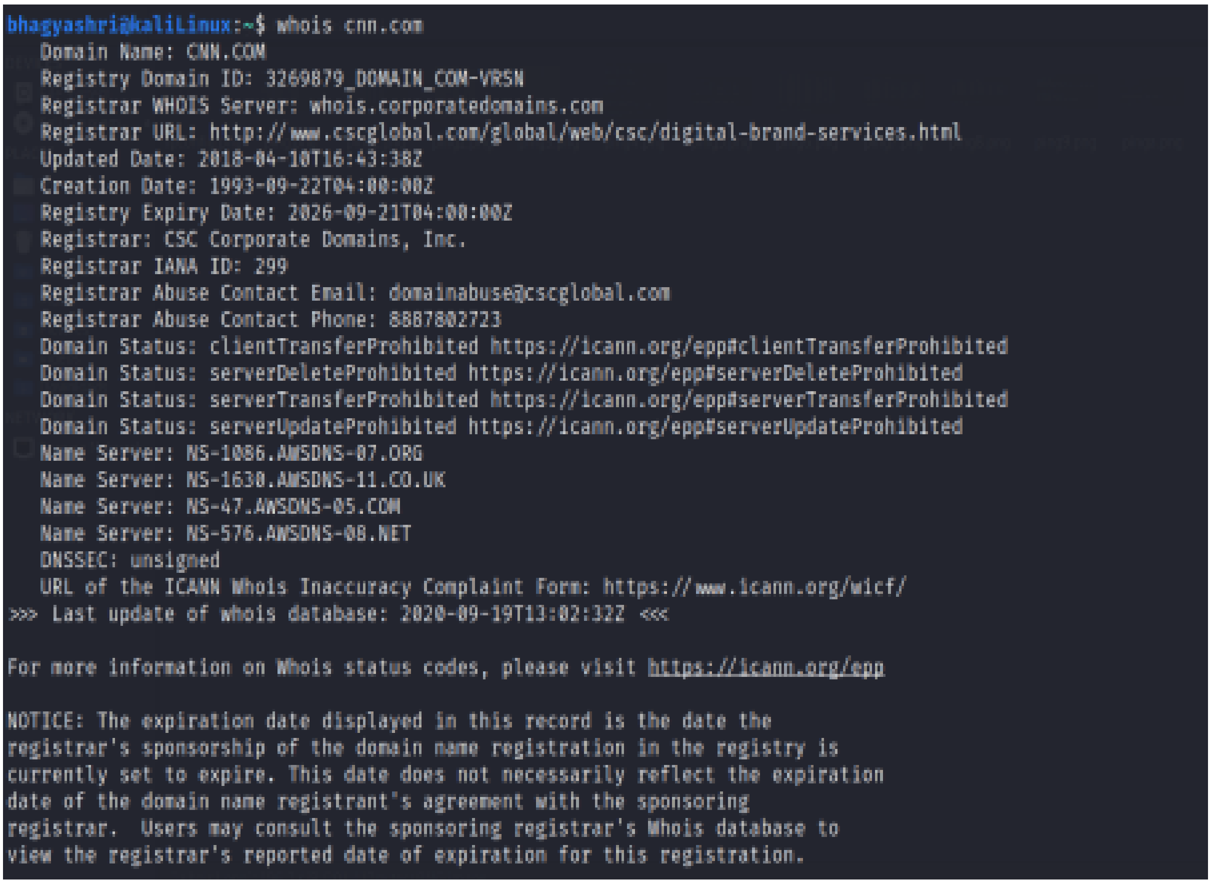
```
bhagyashri@kaliLinux:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-I                     query whois.iana.org and follow its referral
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
```



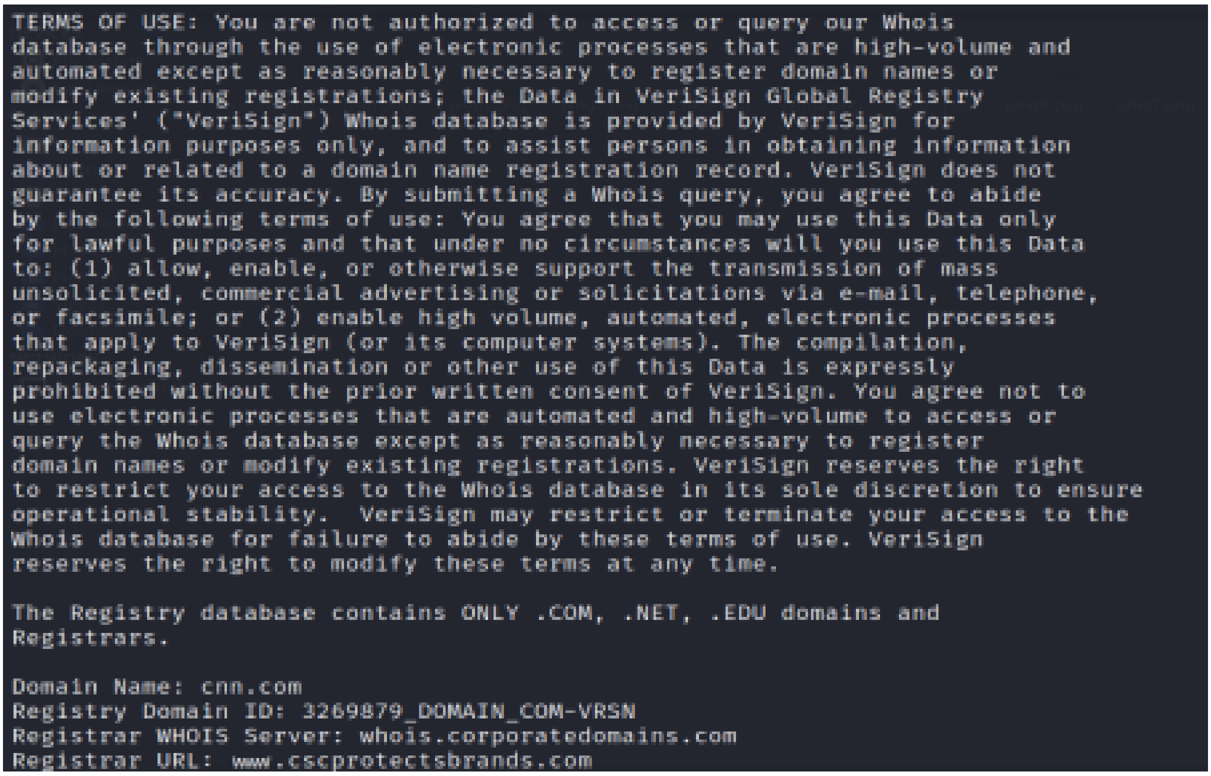
```
-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-I                     query whois.iana.org and follow its referral
-H                     hide legal disclaimers
      --verbose        explain what is being done
      --help           display this help and exit
      --version        output version information and exit

These flags are supported by whois.ripe.net and some RIPE-like servers:
-l                     find the one level less specific match
-L                     find all levels less specific matches
-m                     find all one level more specific matches
-M                     find all levels of more specific matches
-c                     find the smallest match containing a mnt-irt attribute
-x                     exact match
-b                     return brief IP address ranges with abuse contact
-B                     turn off object filtering (show email addresses)
-G                     turn off grouping of associated objects
-d                     return DNS reverse delegation objects too
-i ATTR[,ATTR] ...     do an inverse look-up for specified ATTRibutes
-T TYPE[,TYPE] ...     only look for objects of TYPE
-K                     only primary keys are returned
-r                     turn off recursive look-ups for contact information
-R                     force to show local copy of the domain object even
                       if it contains referral
-a                     also search all the mirrored databases
-s SOURCE[,SOURCE] ... search the database mirrored from SOURCE
-g SOURCE:FIRST-LAST   find updates from SOURCE from serial FIRST to LAST
-t TYPE                request template for object of TYPE
-v TYPE                request verbose template for object of TYPE
-q [version|sources|types]  query specified server info
```

CNS (Roll_50)

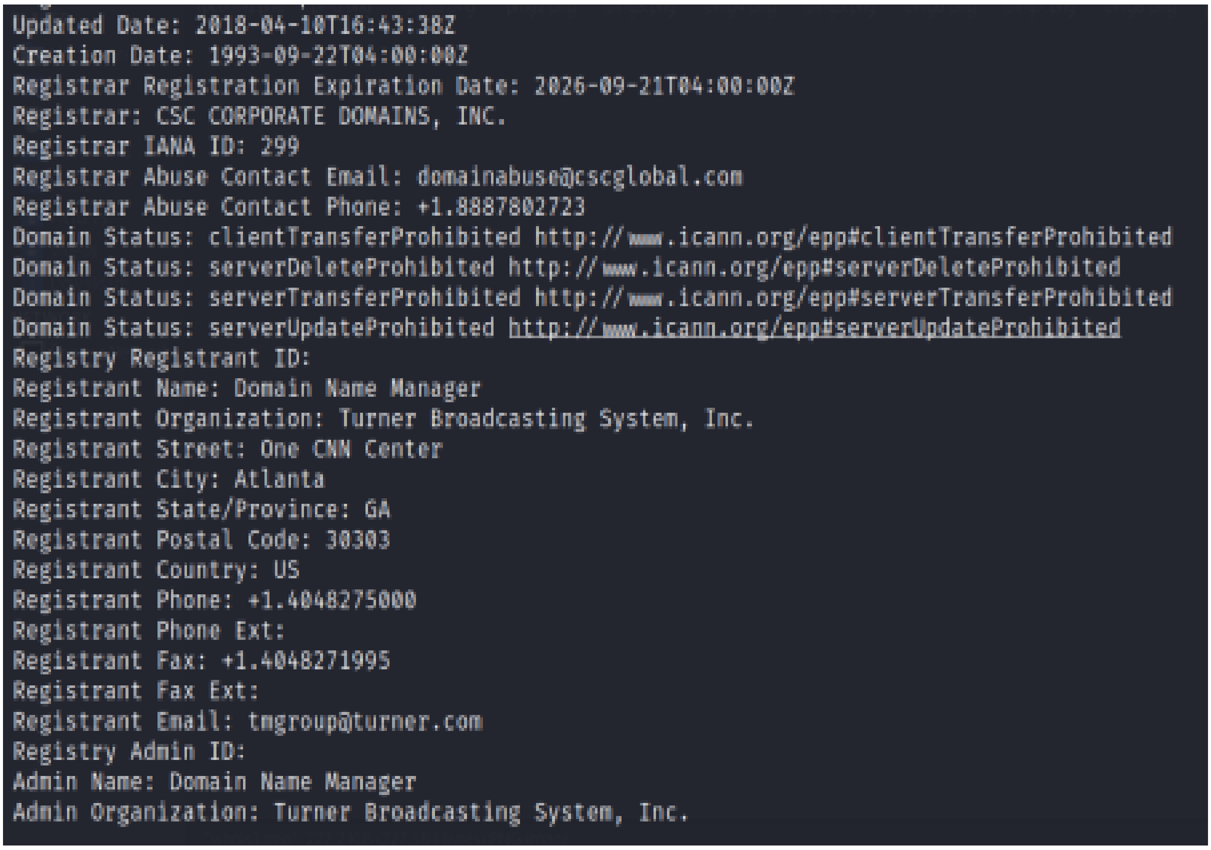
## 9. whois cnn.com



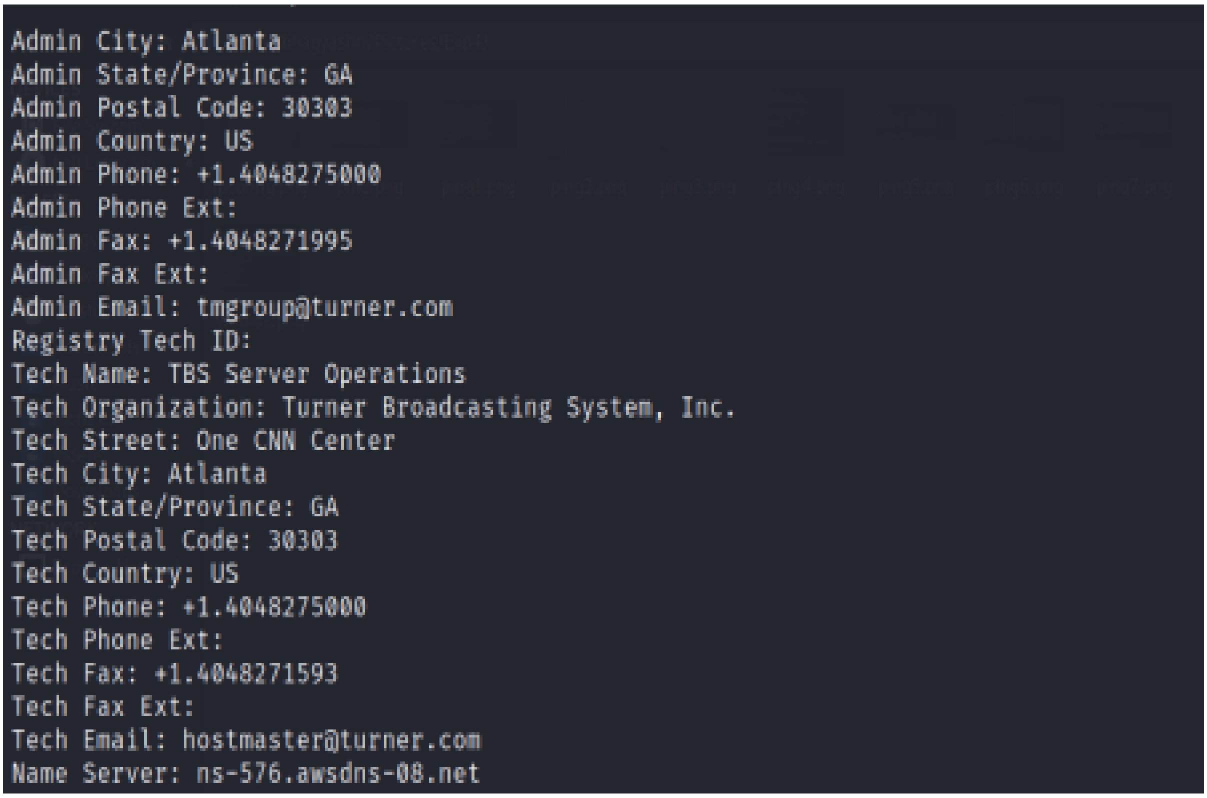
```
bhagyashri@kaliLinux:~$ whois cnn.com
   Domain Name: CNN.COM
   Registry Domain ID: 3269879_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://www.cscglobal.com/global/web/csc/digital-brand-services.html
   Updated Date: 2018-04-10T16:43:38Z
   Creation Date: 1993-09-22T04:00:00Z
   Registry Expiry Date: 2026-09-21T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   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: NS-1086.AWSDNS-07.ORG
   Name Server: NS-1630.AWSDNS-11.CO.UK
   Name Server: NS-47.AWSDNS-05.COM
   Name Server: NS-576.AWSDNS-08.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-09-19T13:02:32Z <<<

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.
```



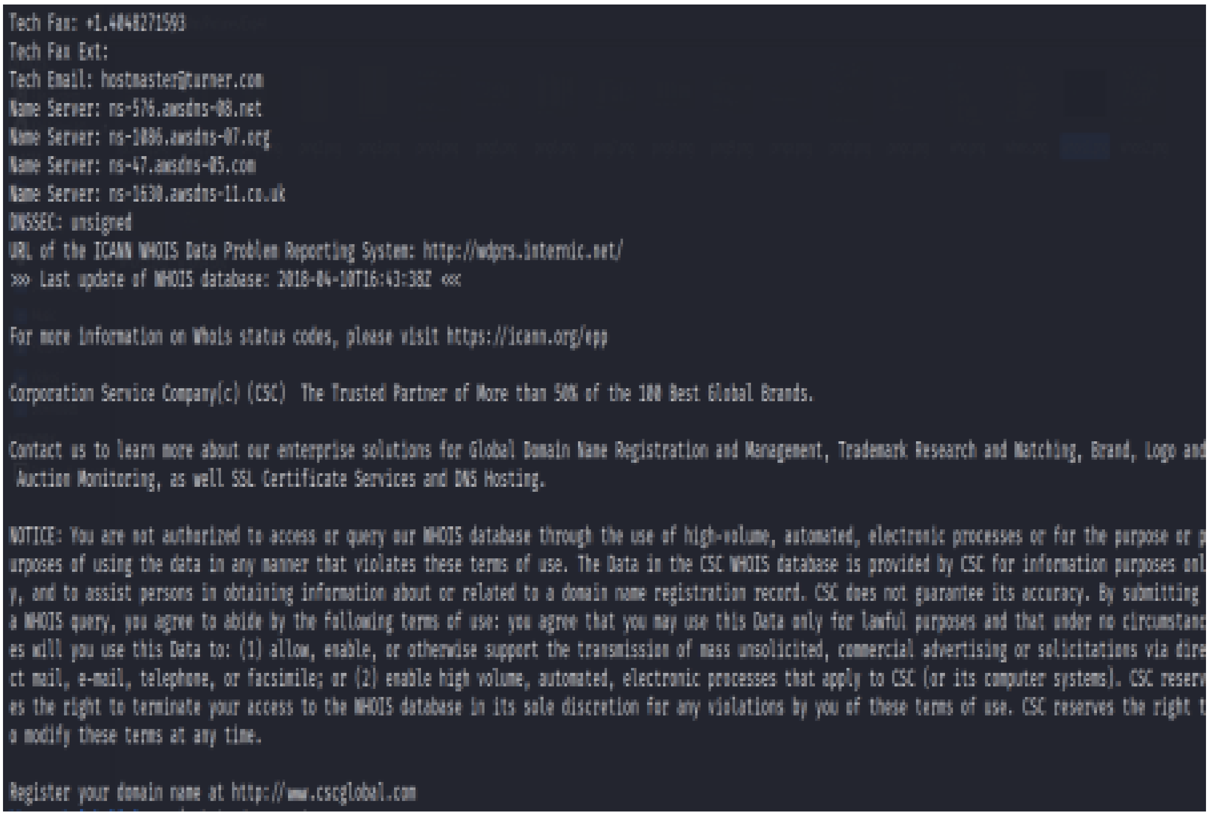
```
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") 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.

Domain Name: cnn.com
Registry Domain ID: 3269879_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
```



```
Updated Date: 2018-04-10T16:43:38Z
Creation Date: 1993-09-22T04:00:00Z
Registrar Registration Expiration Date: 2026-09-21T04:00:00Z
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverDeleteProhibited http://www.icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited http://www.icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited http://www.icann.org/epp#serverUpdateProhibited
Registry Registrant ID:
Registrant Name: Domain Name Manager
Registrant Organization: Turner Broadcasting System, Inc.
Registrant Street: One CNN Center
Registrant City: Atlanta
Registrant State/Province: GA
Registrant Postal Code: 30303
Registrant Country: US
Registrant Phone: +1.4048275000
Registrant Phone Ext:
Registrant Fax: +1.4048271995
Registrant Fax Ext:
Registrant Email: tmgroup@turner.com
Registry Admin ID:
Admin Name: Domain Name Manager
Admin Organization: Turner Broadcasting System, Inc.
```



```
Admin City: Atlanta
Admin State/Province: GA
Admin Postal Code: 30303
Admin Country: US
Admin Phone: +1.4048275000
Admin Phone Ext:
Admin Fax: +1.4048271995
Admin Fax Ext:
Admin Email: tmgroup@turner.com
Registry Tech ID:
Tech Name: TBS Server Operations
Tech Organization: Turner Broadcasting System, Inc.
Tech Street: One CNN Center
Tech City: Atlanta
Tech State/Province: GA
Tech Postal Code: 30303
Tech Country: US
Tech Phone: +1.4048275000
Tech Phone Ext:
Tech Fax: +1.4048271593
Tech Fax Ext:
Tech Email: hostmaster@turner.com
Name Server: ns-576.awsdns-08.net
```



```
Tech Fax: +1.4048271593
Tech Fax Ext:
Tech Email: hostmaster@turner.com
Name Server: ns-576.awsdns-08.net
Name Server: ns-1086.awsdns-07.org
Name Server: ns-47.awsdns-05.com
Name Server: ns-1630.awsdns-11.co.uk
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2018-04-10T16:43:38Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Corporation Service Company(c) (CSC)  The Trusted Partner of More than 50% of the 100 Best Global Brands.

Contact us to learn more about our enterprise solutions for Global Domain Name Registration and Management, Trademark Research and Watching, Brand, Logo and
 Auction Monitoring, as well SSL Certificate Services and DNS Hosting.

NOTICE: You are not authorized to access or query our WHOIS database through the use of high-volume, automated, electronic processes or for the purpose or p
urposes of using the data in any manner that violates these terms of use. The Data in the CSC WHOIS database is provided by CSC for information purposes onl
y, and to assist persons in obtaining information about or related to a domain name registration record. CSC 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 circumstanc
es will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via dire
ct mail, e-mail, telephone, or facsimile; or (2) enable high volume, automated, electronic processes that apply to CSC (or its computer systems). CSC reserv
es the right to terminate your access to the WHOIS database in its sole discretion for any violations by you of these terms of use. CSC reserves the right t
o modify these terms at any time.

Register your domain name at http://www.cscglobal.com
```

## 10. host

11. host www.google.com

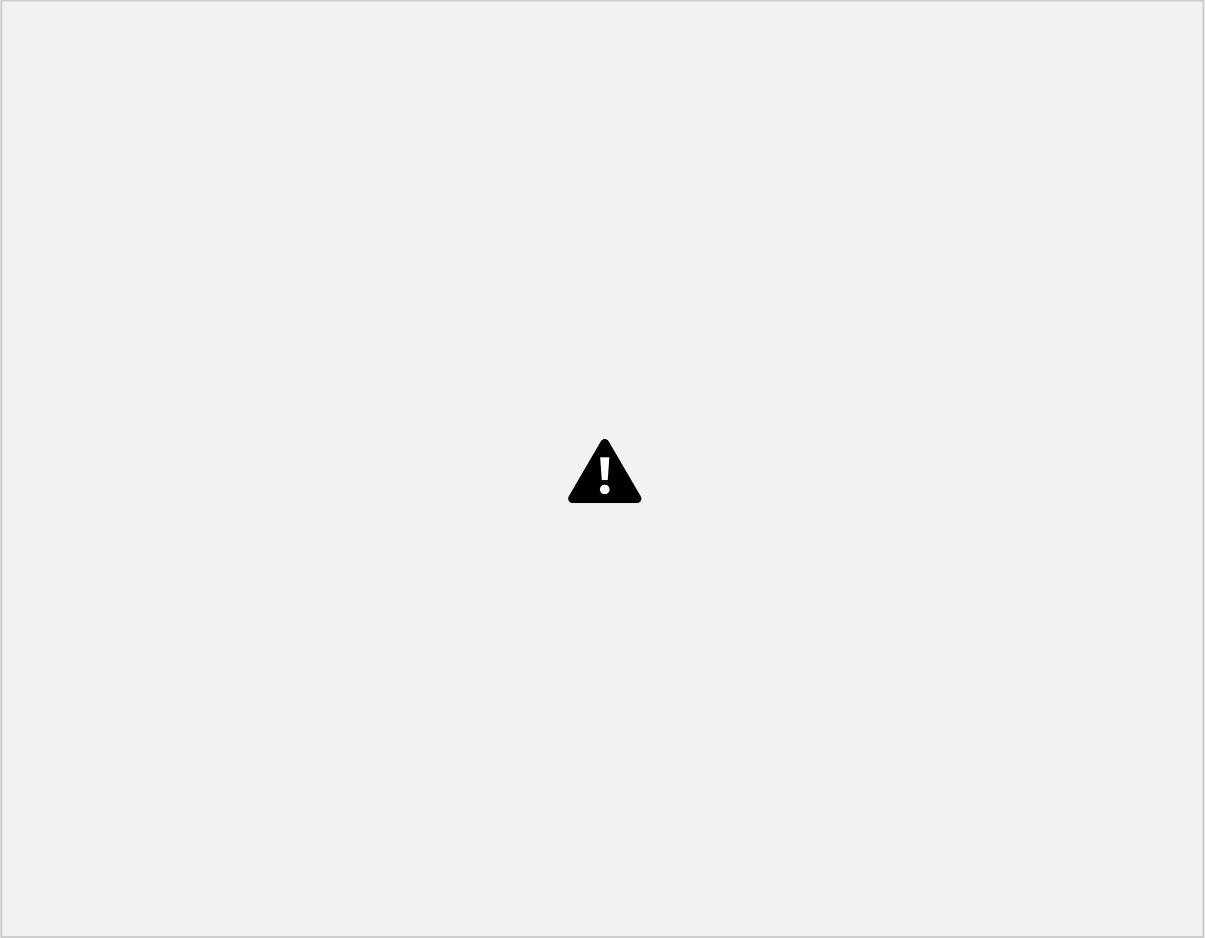
12. host -t CNAME www.redhat.com

13. hostname

14. hostname -a [ no alias name for my system so blank o/p]

15. Dig

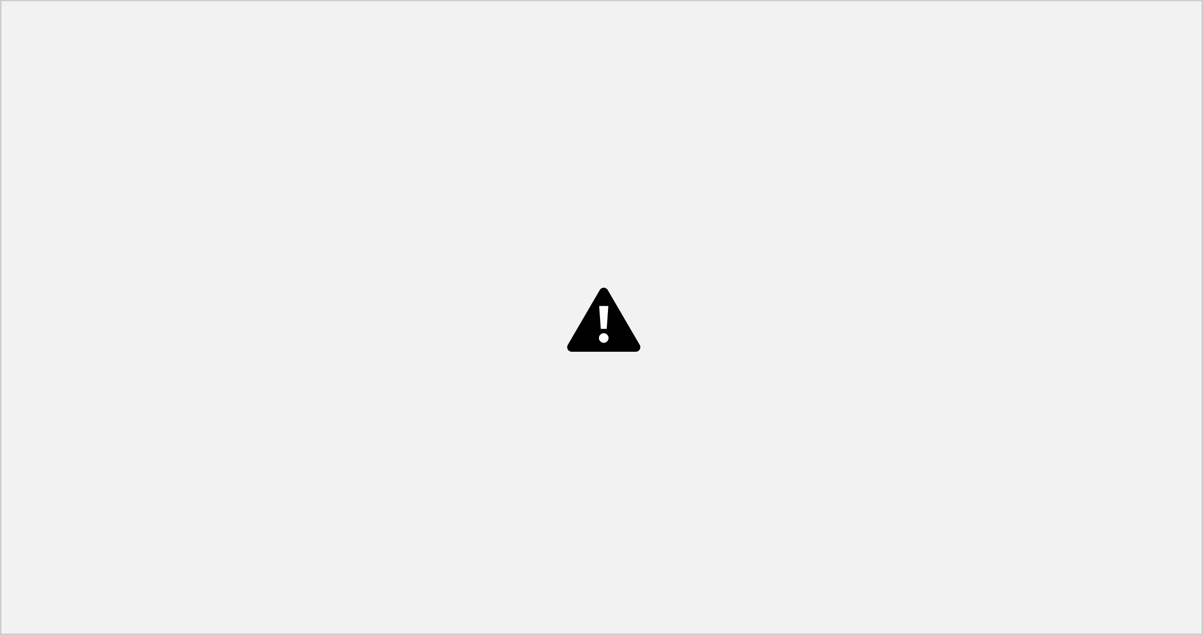
- dig



- dig google.com ANY +noall +answer

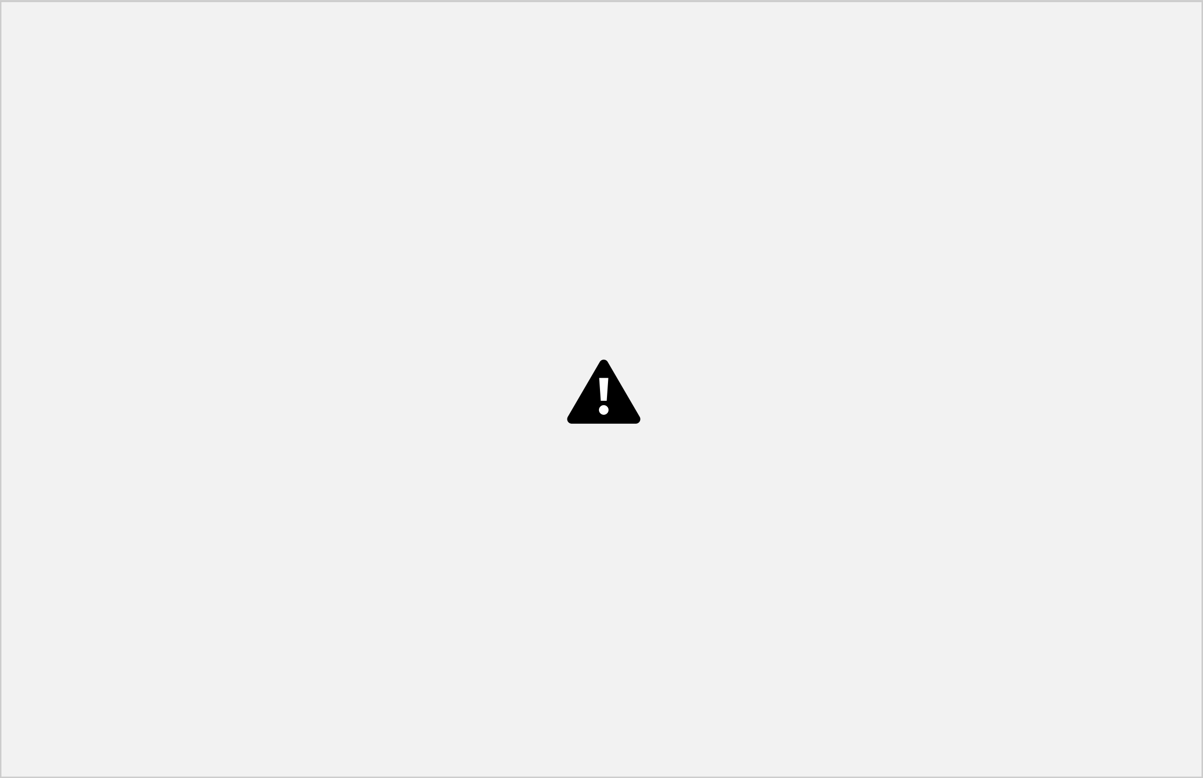
- dig google.com mx +noall +answer redhat.com ns +noall +answer

- dig dmce.ac.in

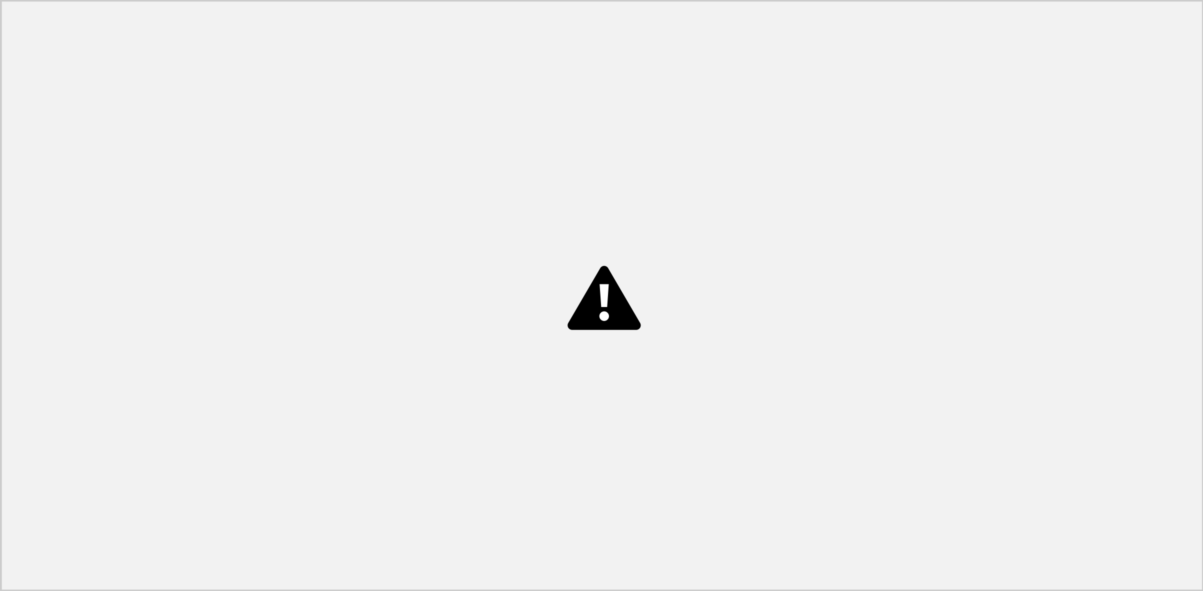


- dig -x 172.217.166.46 +short

- dig google.com MX

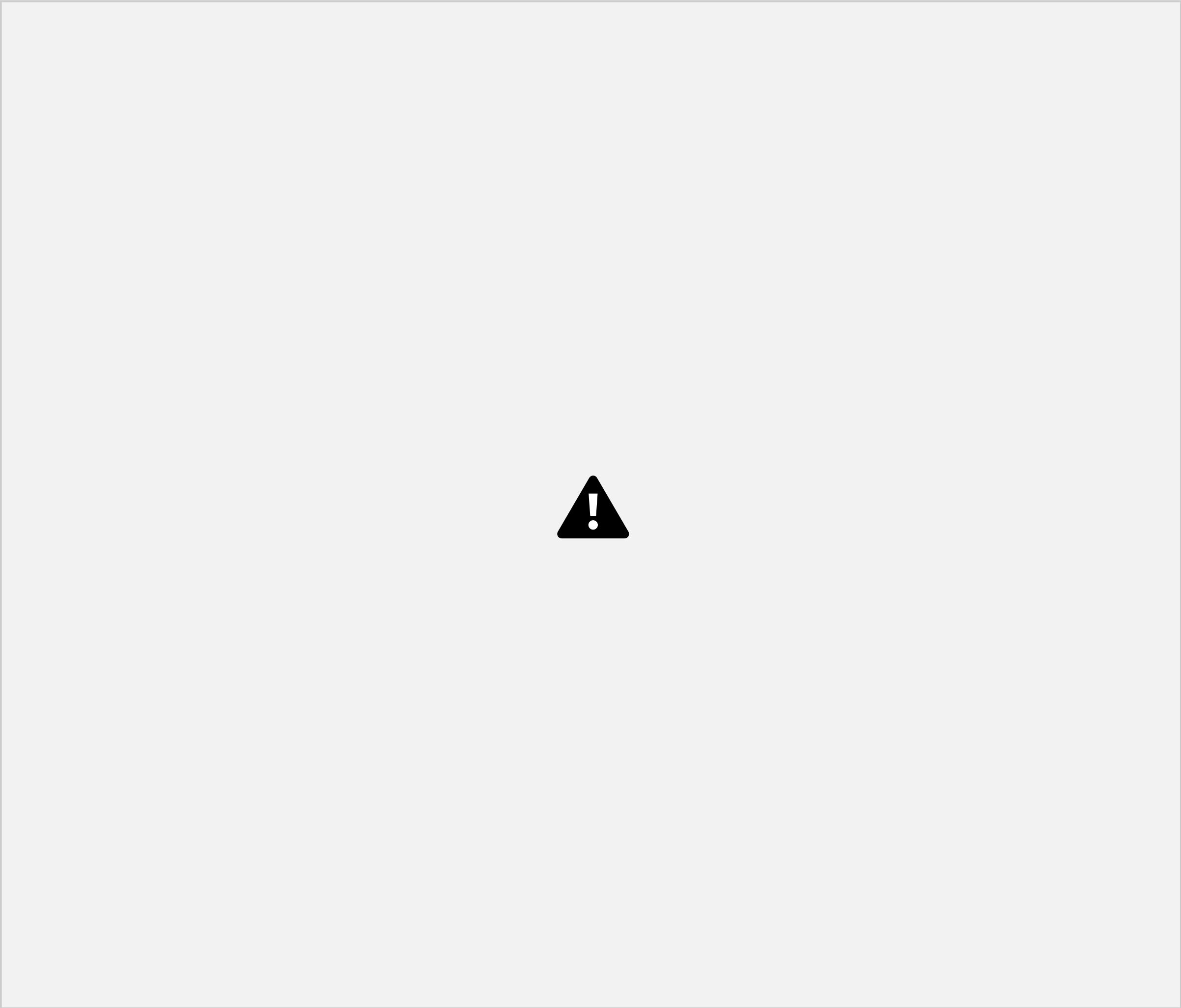


- dig google.com SOA



- dig yahoo.com +short

- dig google.com TTL



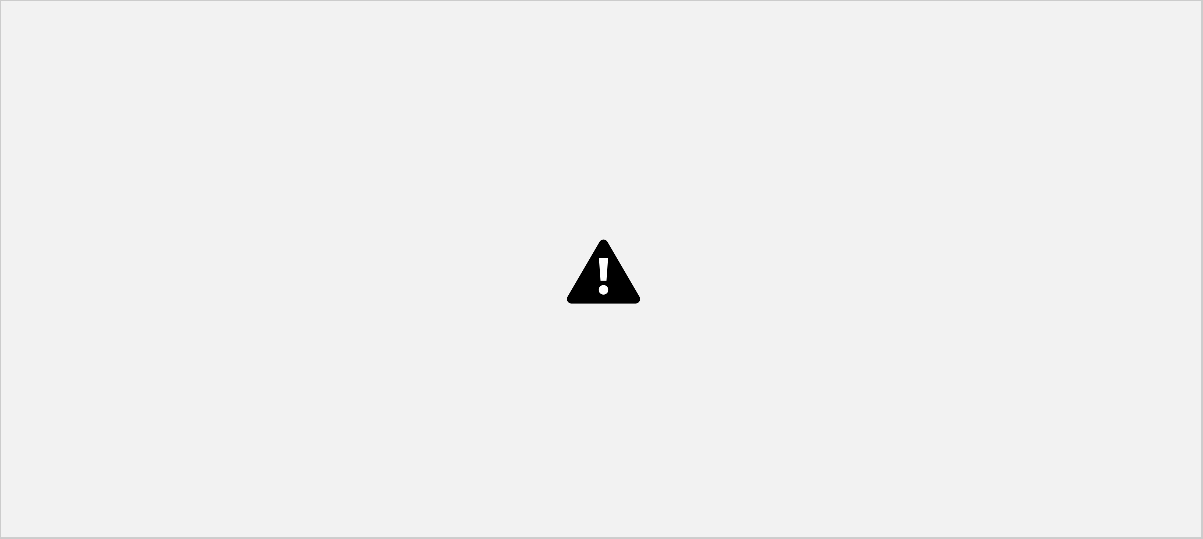
## 16. Ns Lookup

- nslookup amazon.com

- nslookup 52.2.4.26

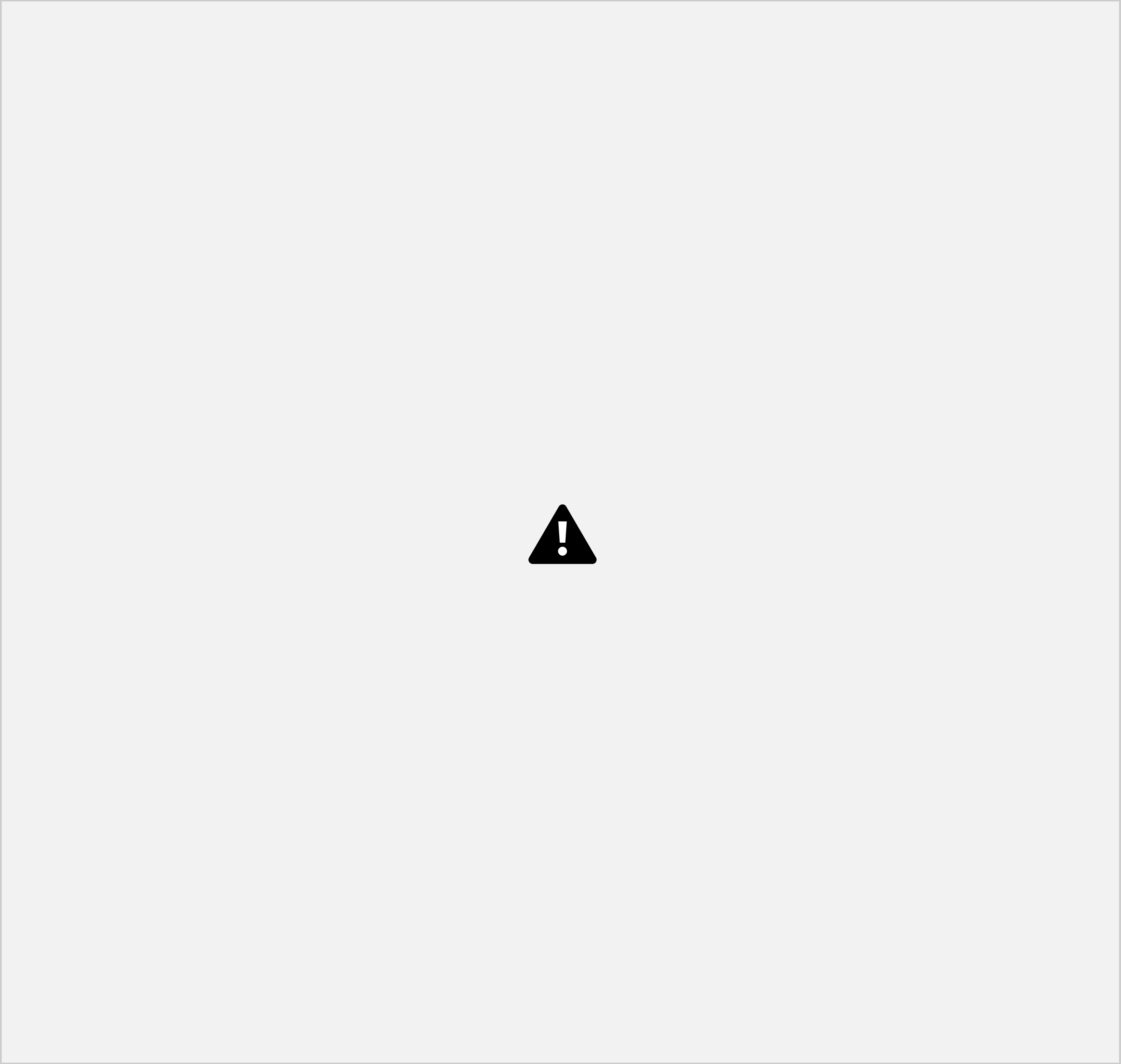
- nslookup -query=mx www.amazon.com

- nslookup -query=ns www.yahoo.com

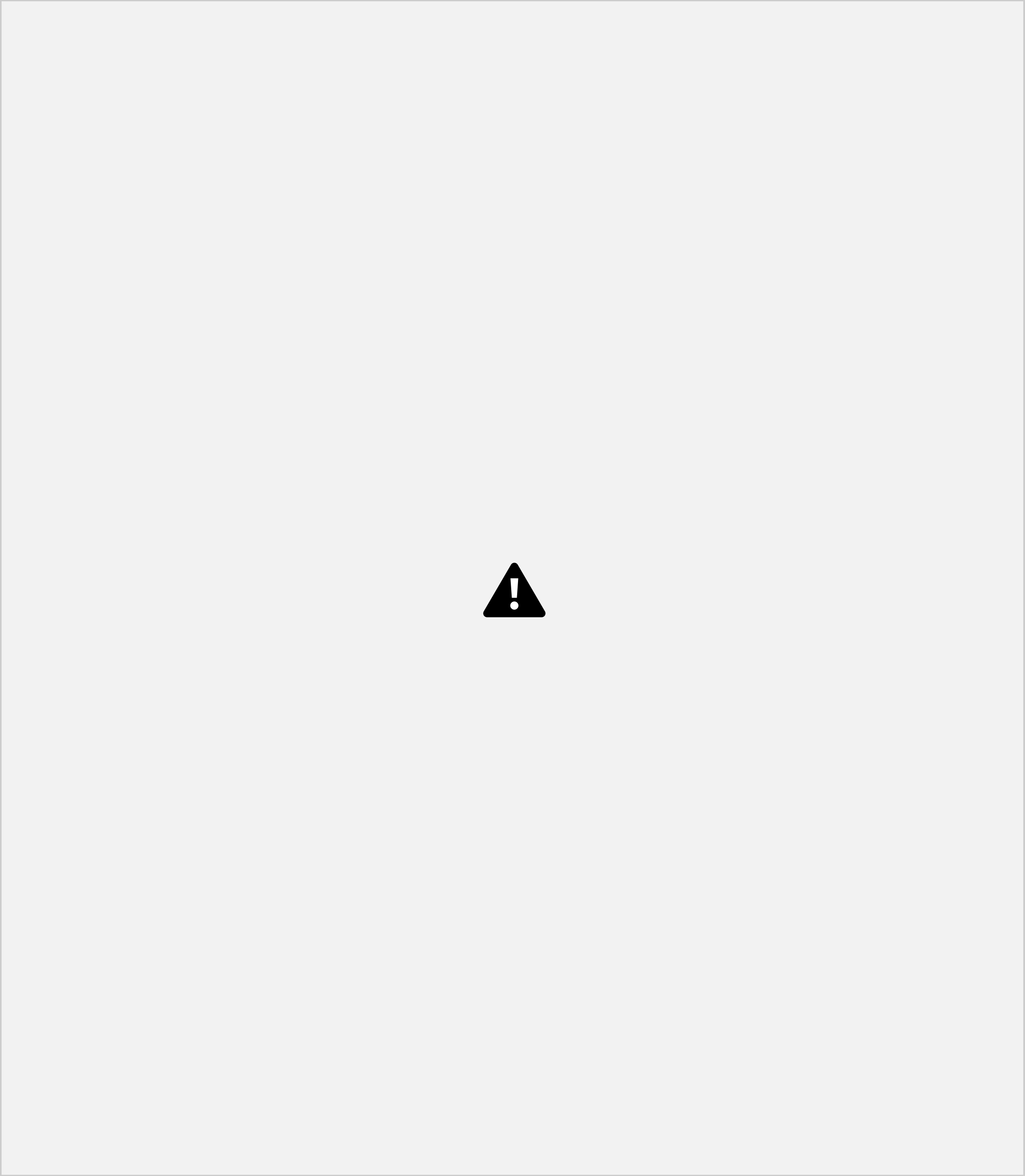


- nslookup -type=soa www.yahoo.com

- nslookup -query=any yahoo.com



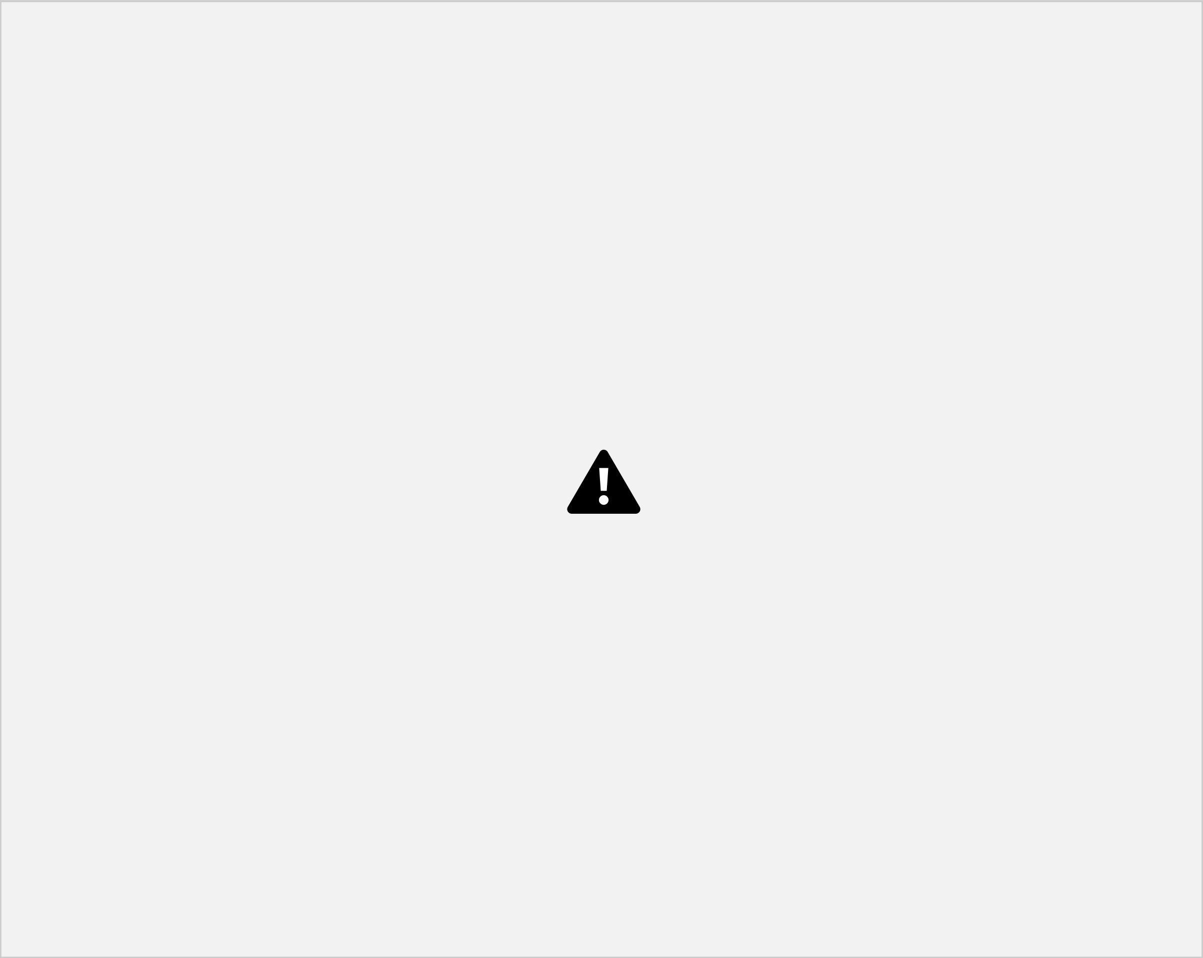
- nslookup -debug yahoo.com



CNS (Roll_50)

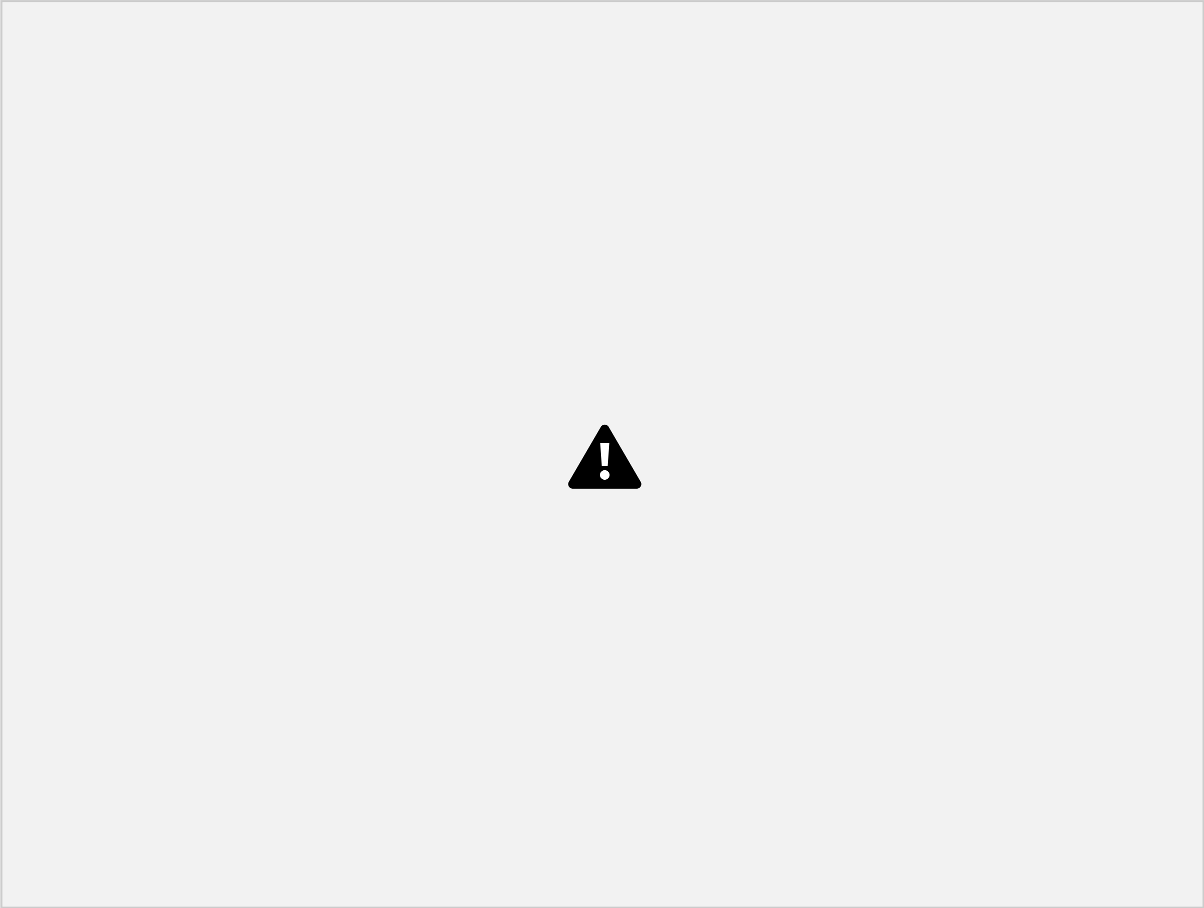
## 17. Netstat

- netstat



- netstat -g

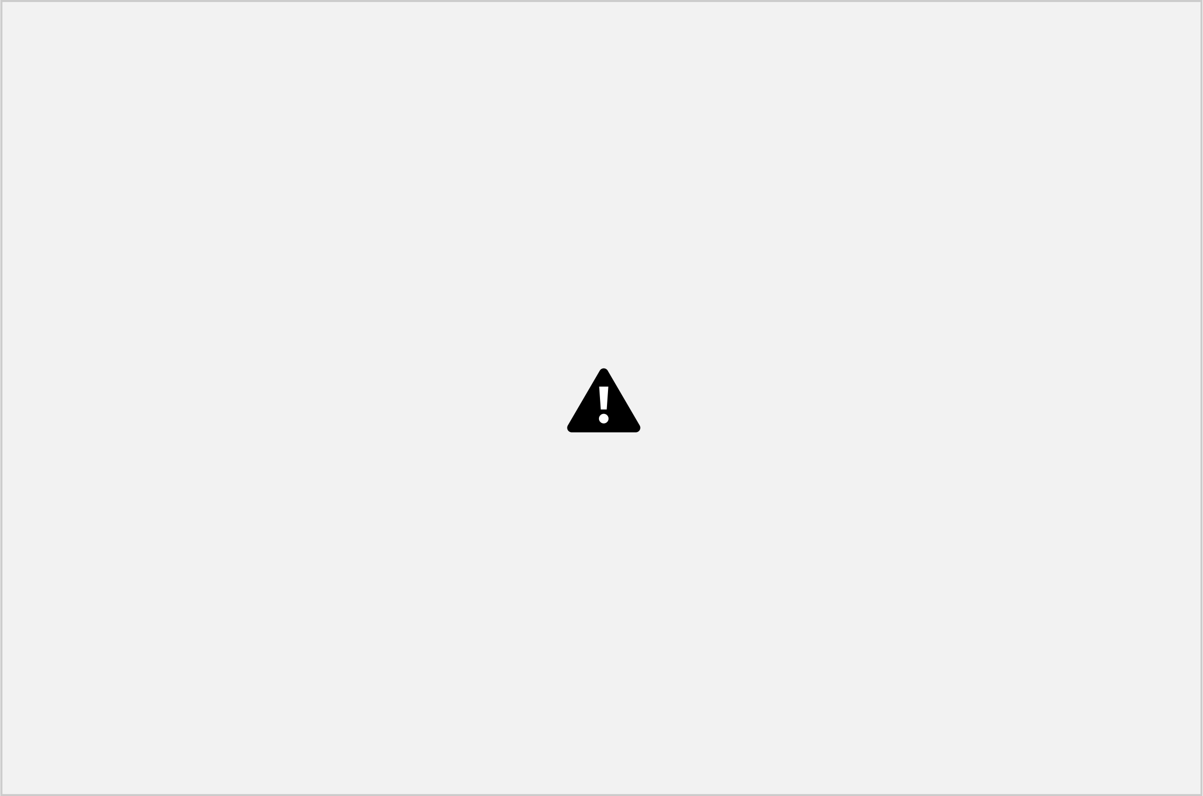
- netstat -a | more



- netstat -ie

- netstat -i

- netstat -l



- netstat -lt

- netstat -lu

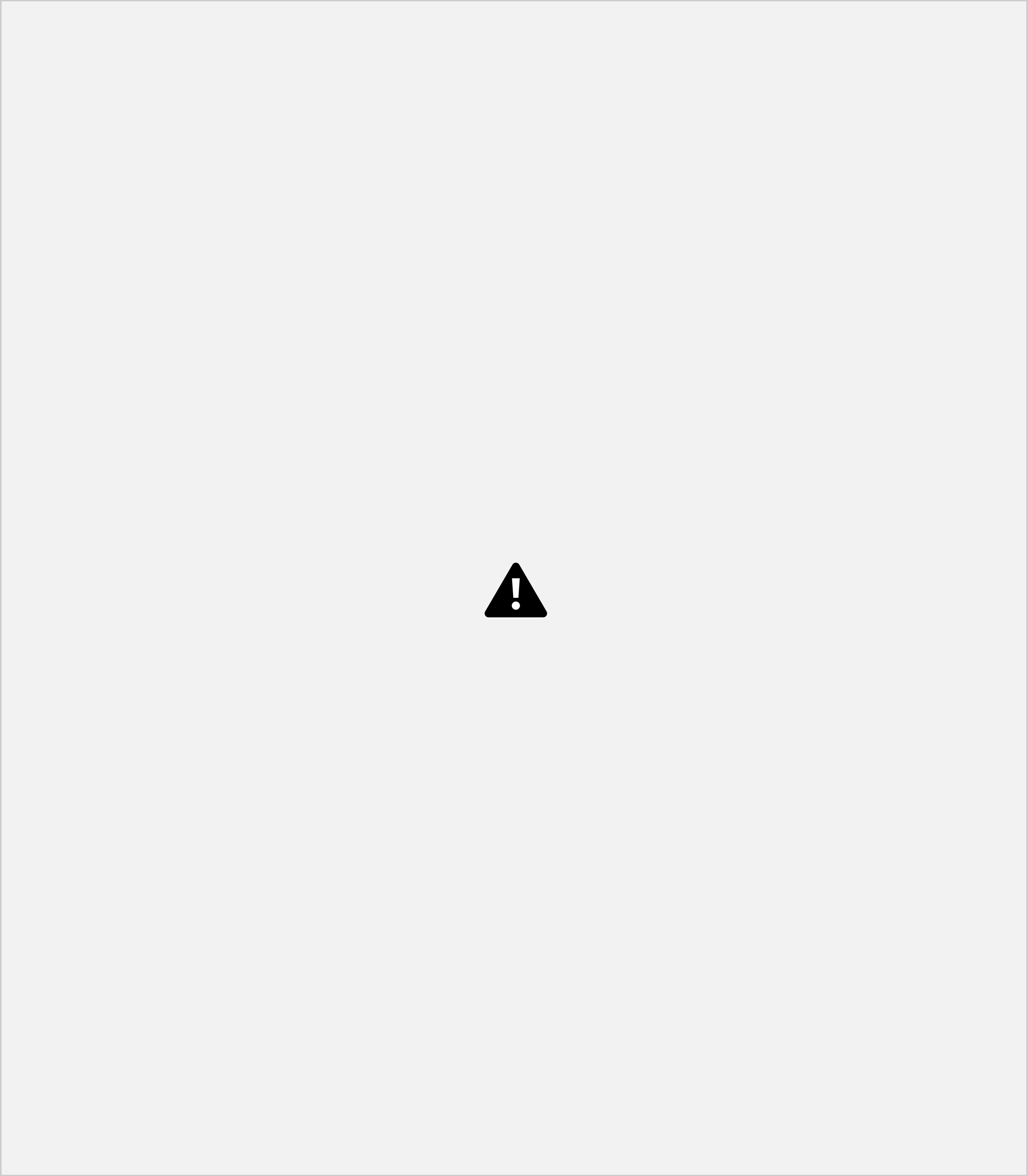
- netstat -at

- netstat -au

- netstat -r

- netstat -c

- netstat -st



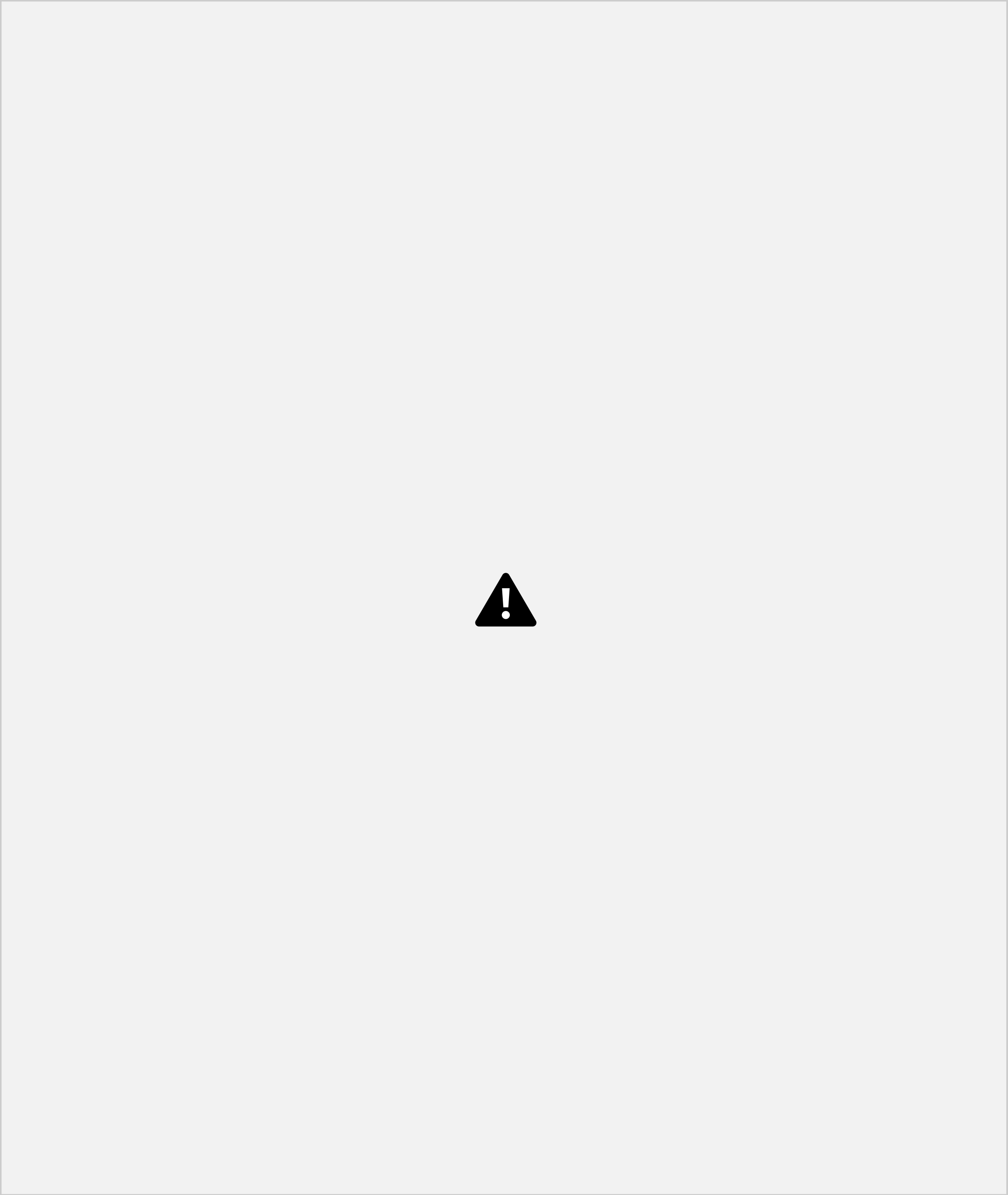
CNS (Roll_50)

- netstat -su

CNS (Roll_50)

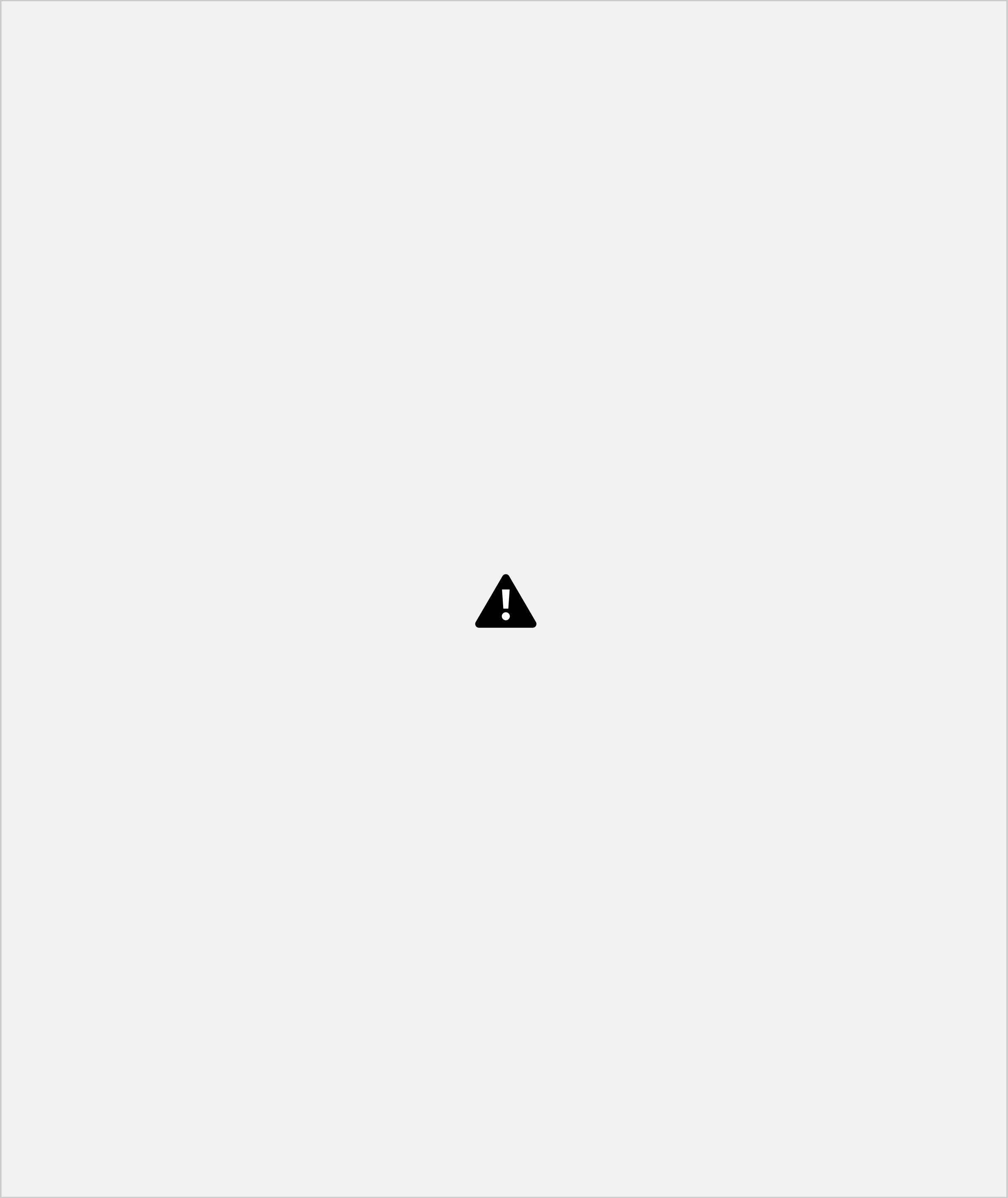
- netstat -s

CNS (Roll_50)



CNS (Roll_50)

- netstat –statistics --raw

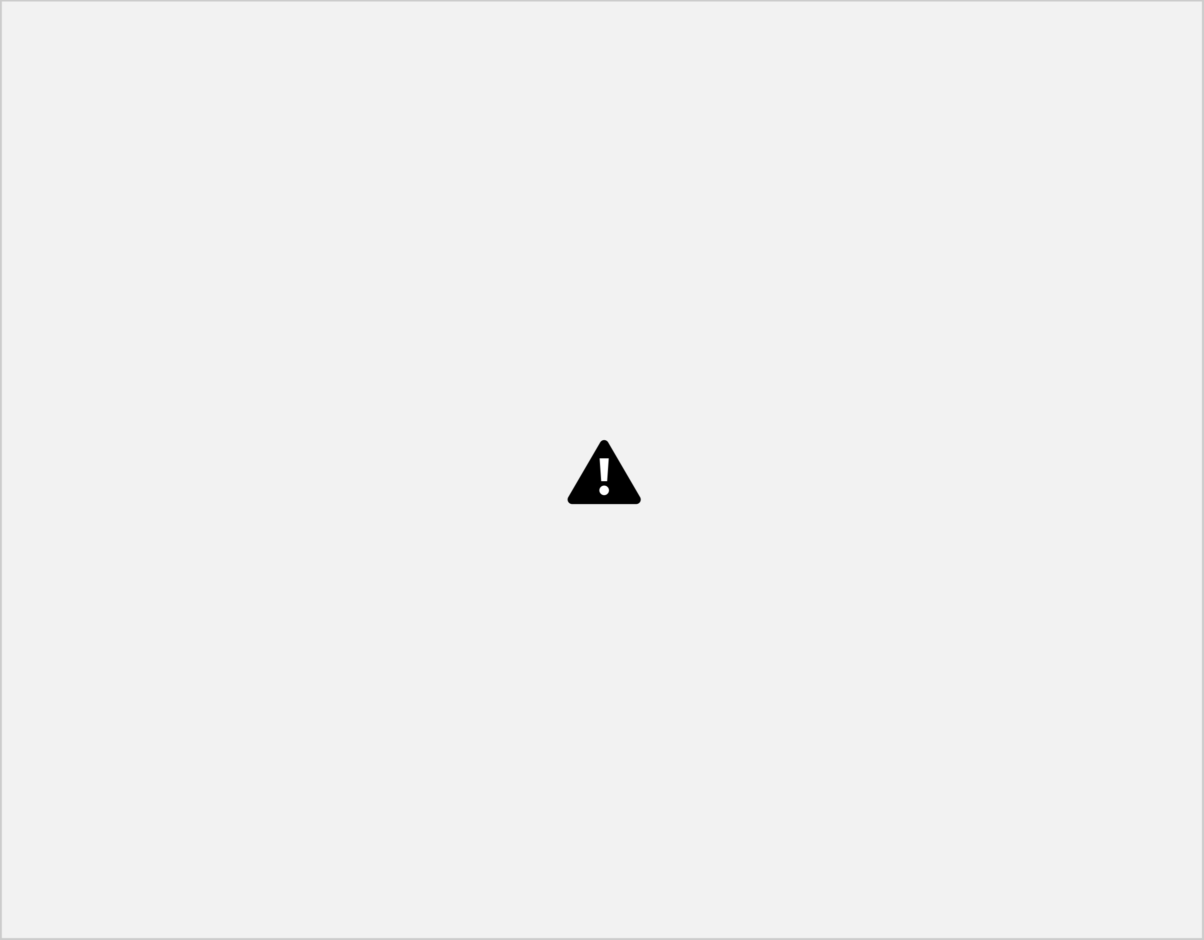


CNS (Roll_50)

- netstat --verbose

CNS (Roll_50)

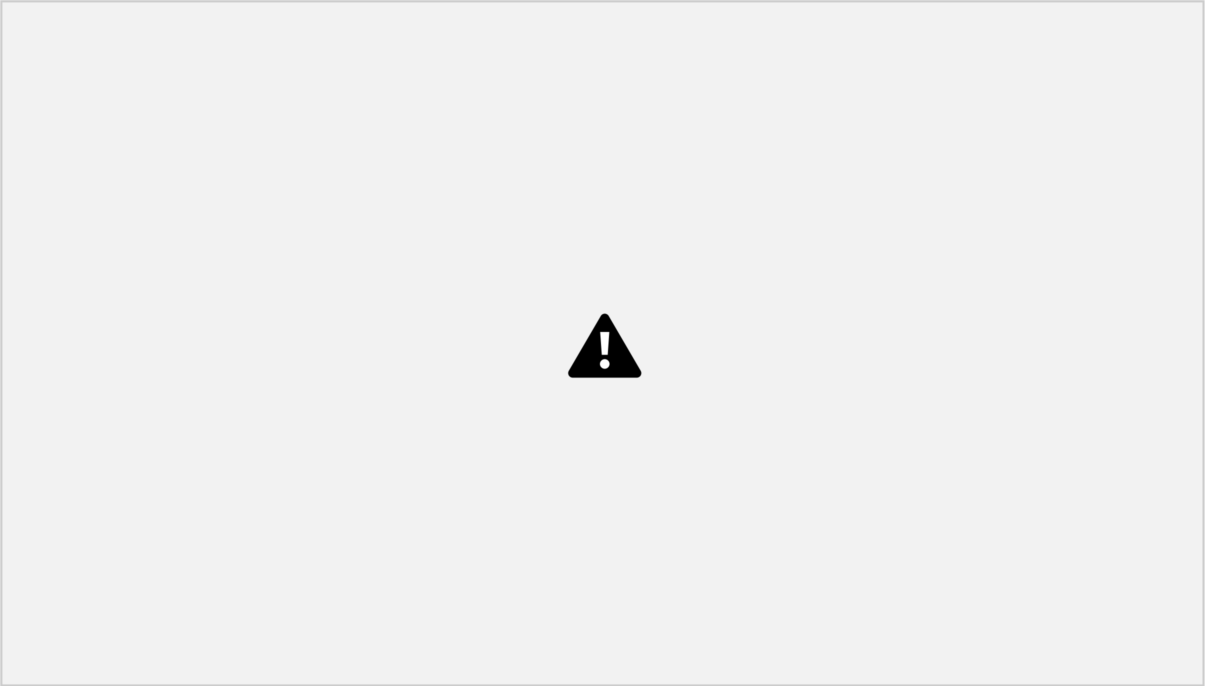
- netstat -ac 5|grep udp



CNS (Roll_50)

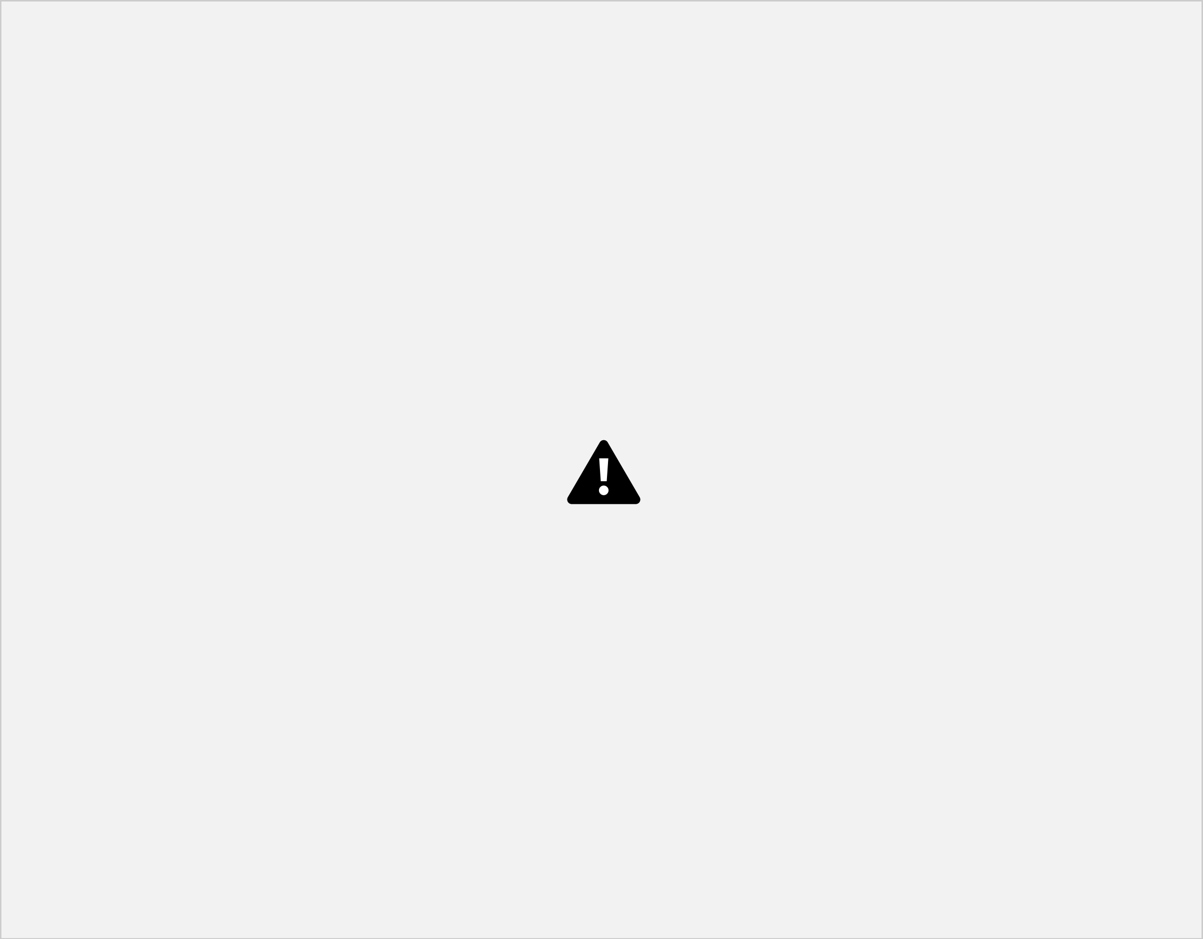
## 18. Ping

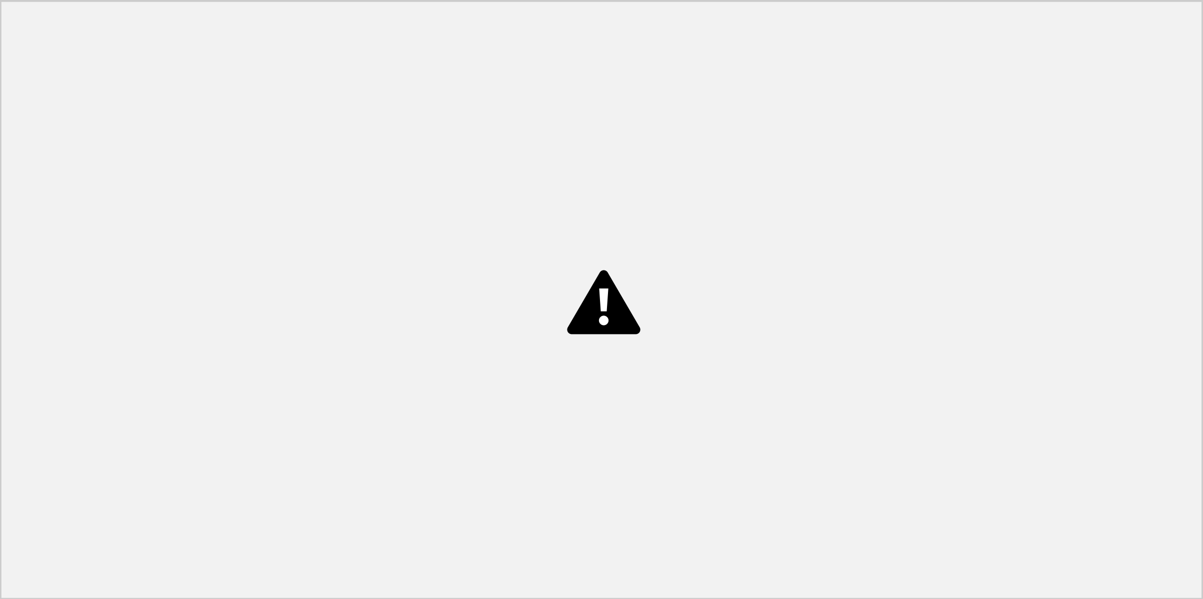
- ping google.com



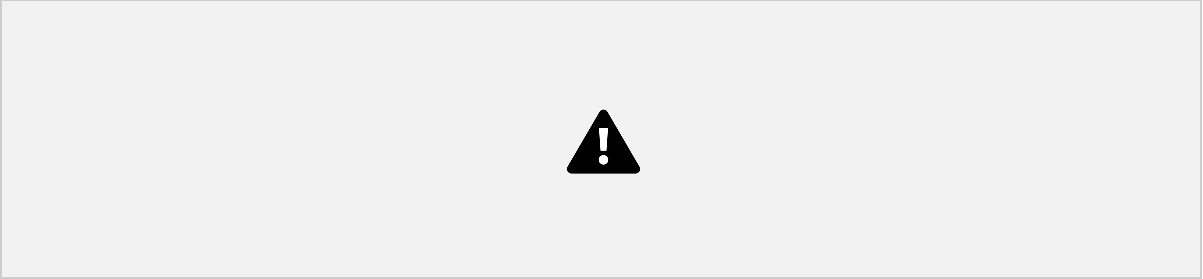
CNS (Roll_50)

- ping 56.90.238.44





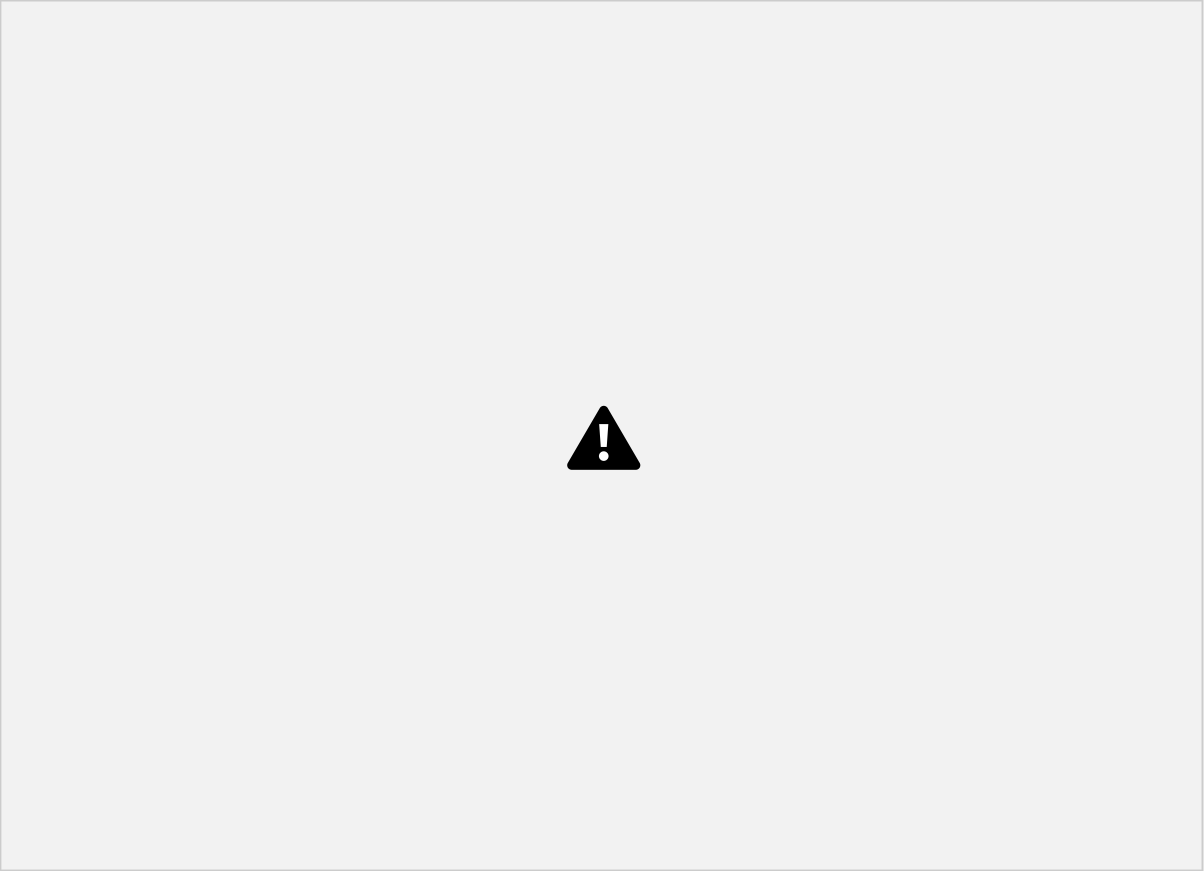
- ping -c 3 amazon.com



Packet 100% loss

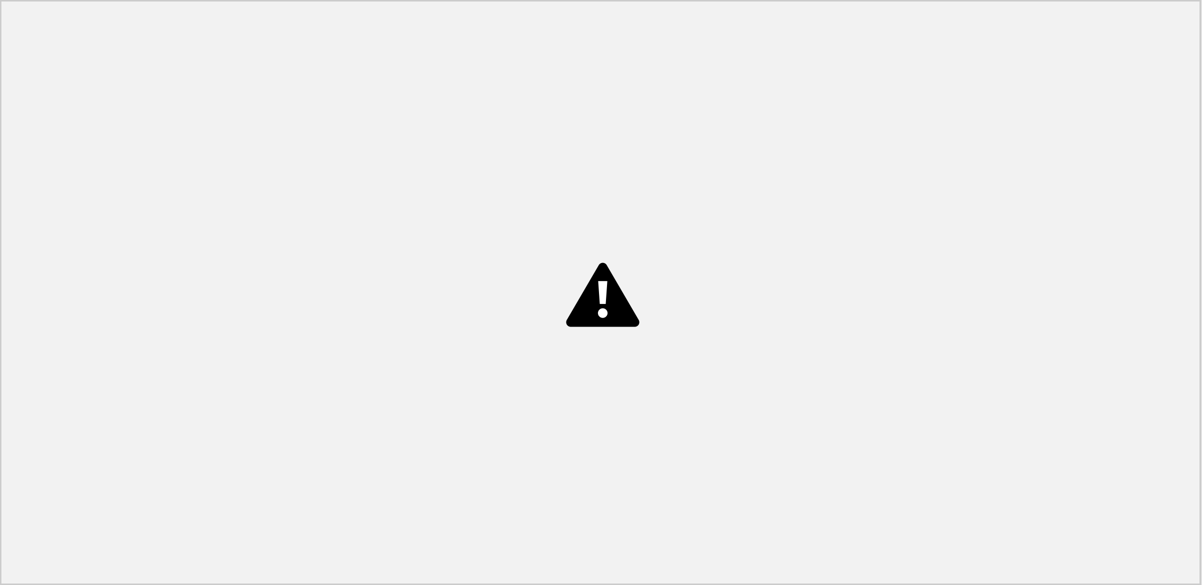
- ping -c 6 163.53.78.87

- ping -v www.google.com



- ping -d www.google.com

- ping -b www.google.com



- ping -s 40 -c 5 amazon.com

- ping -i 2 -c 5 amazon.com

- ping -w 3 www.amazon.com

- ping -f www.flipkart.com

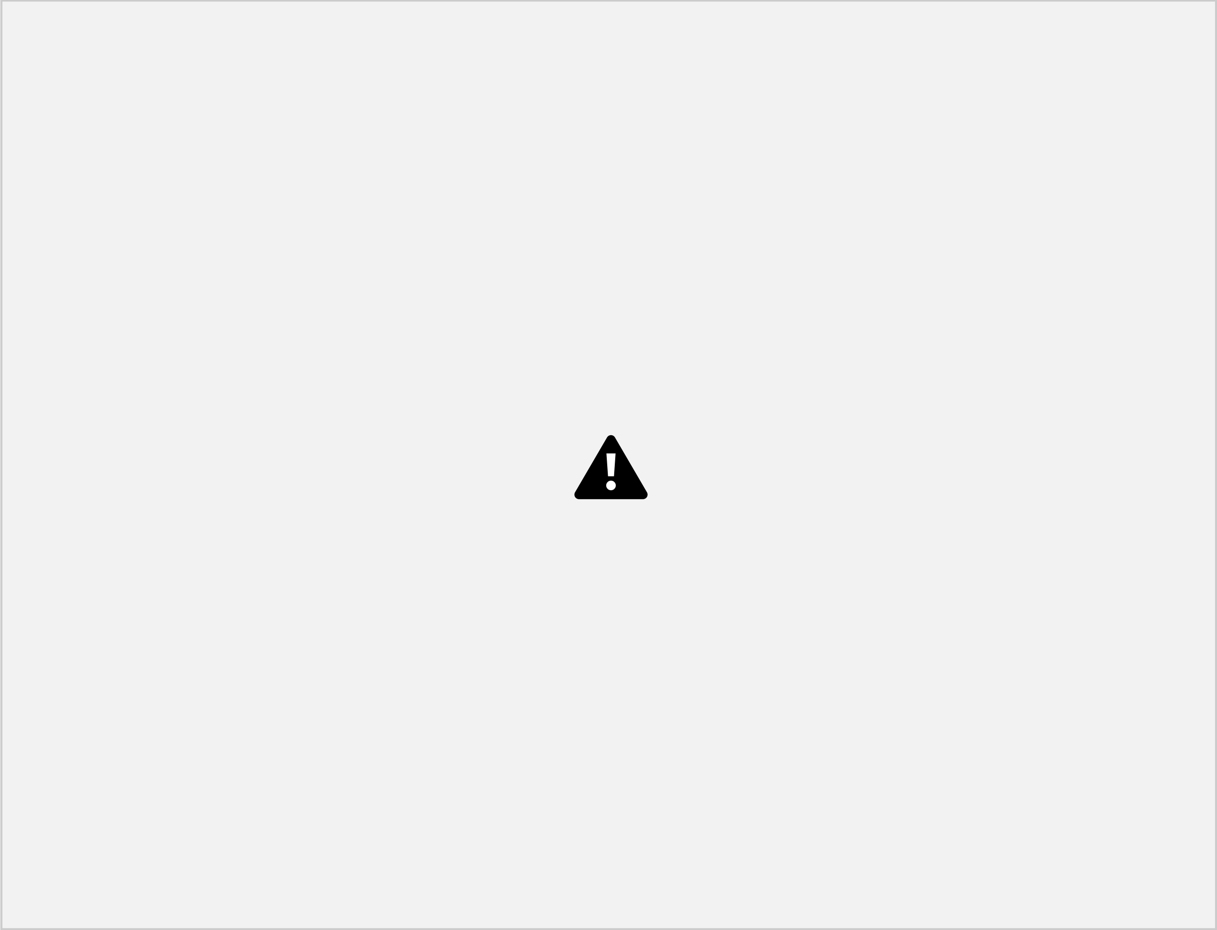
- ping -T tsonly -c 2 127.0.0.1

- ping -T tsandaddr -c 2 127.0.0.1

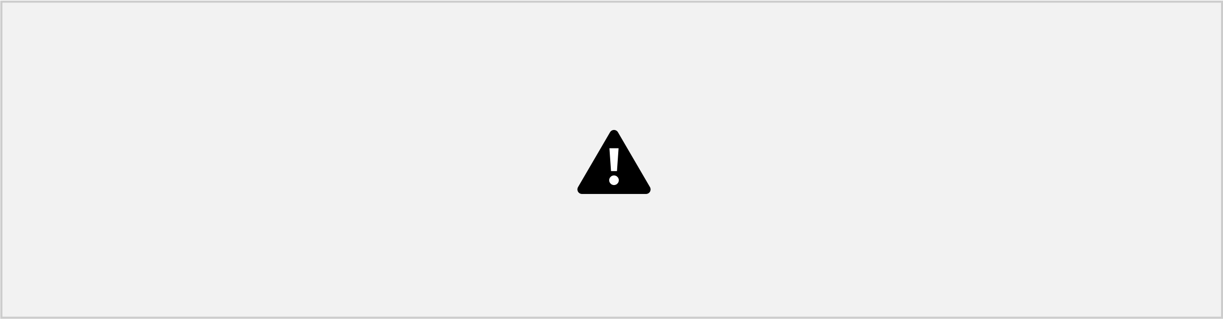
CNS (Roll_50)

## 19. Traceroute

- traceroute

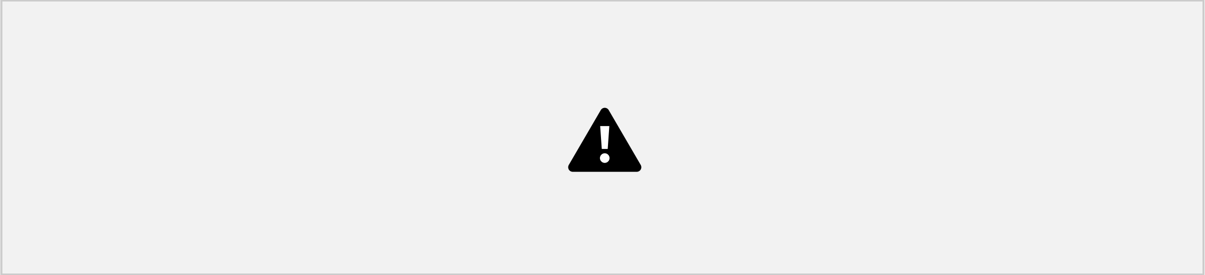


- traceroute -f 25 google.com



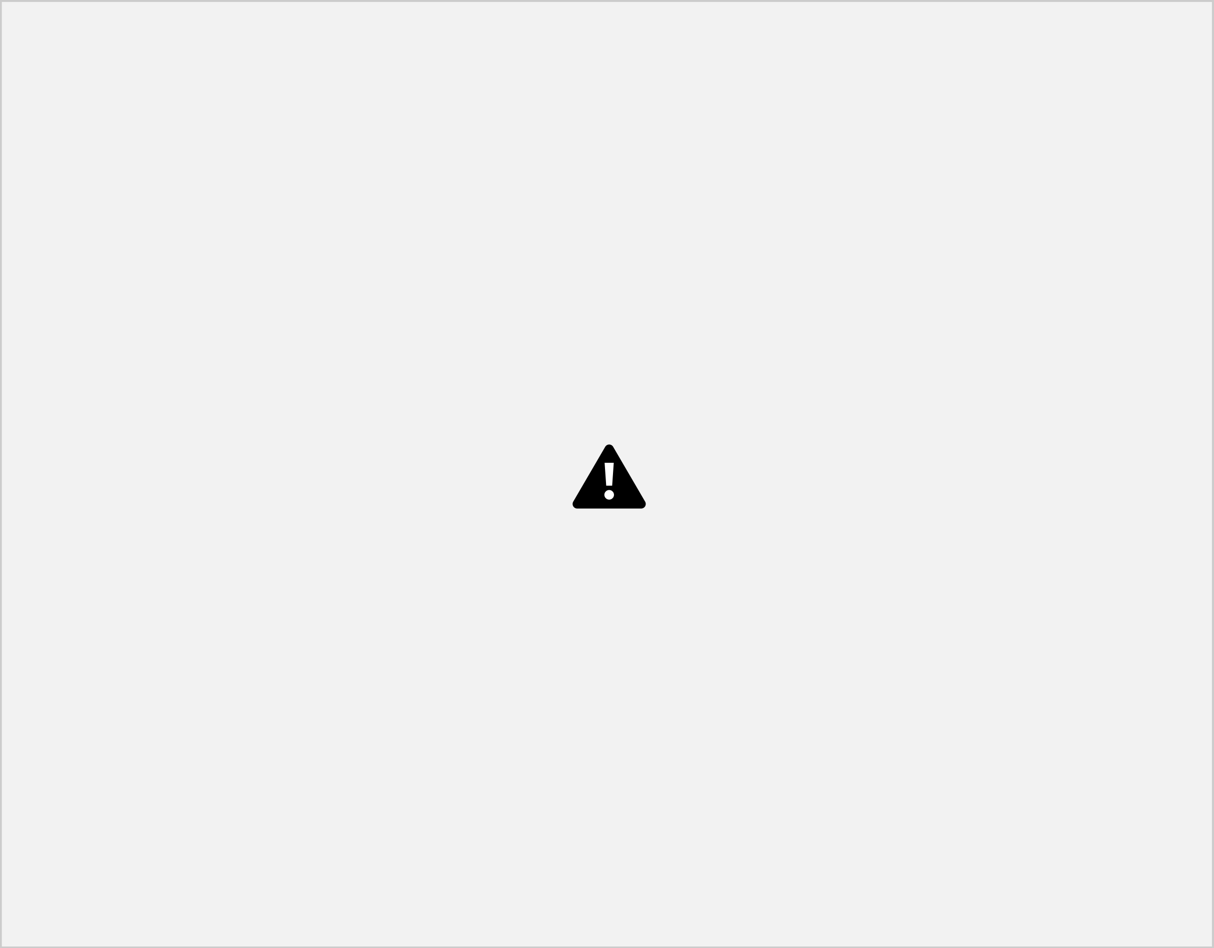
CNS (Roll_50)

- traceroute -m 5 google.com



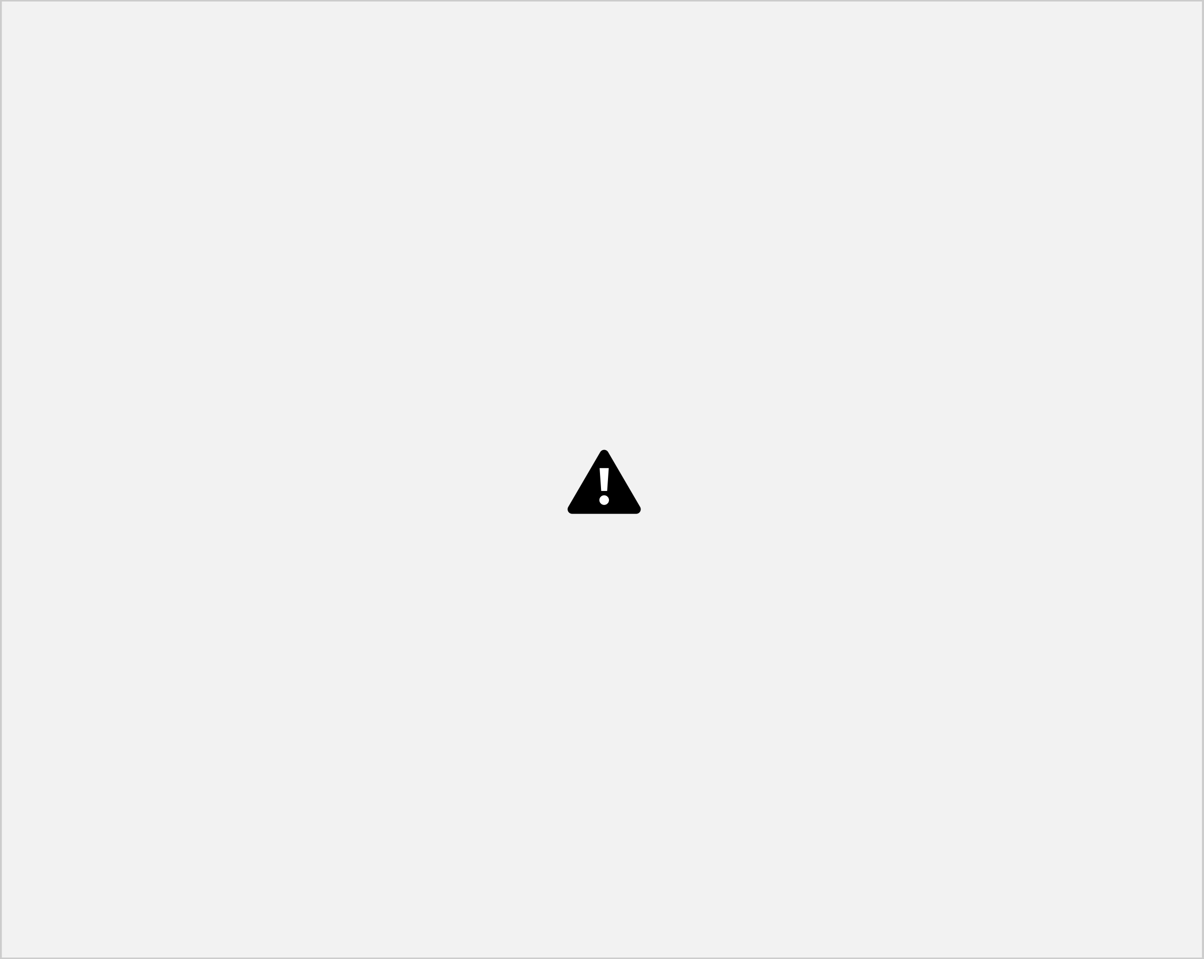
- traceroute -e kaliLinux

- traceroute google.com



CNS (Roll_50)

- traceroute -q 1 google.com



CNS (Roll_50)

## 20. ARP

- arp

- arp -e

- arp -i kaliLinux

- arp -d kaliLinux

- arp -a