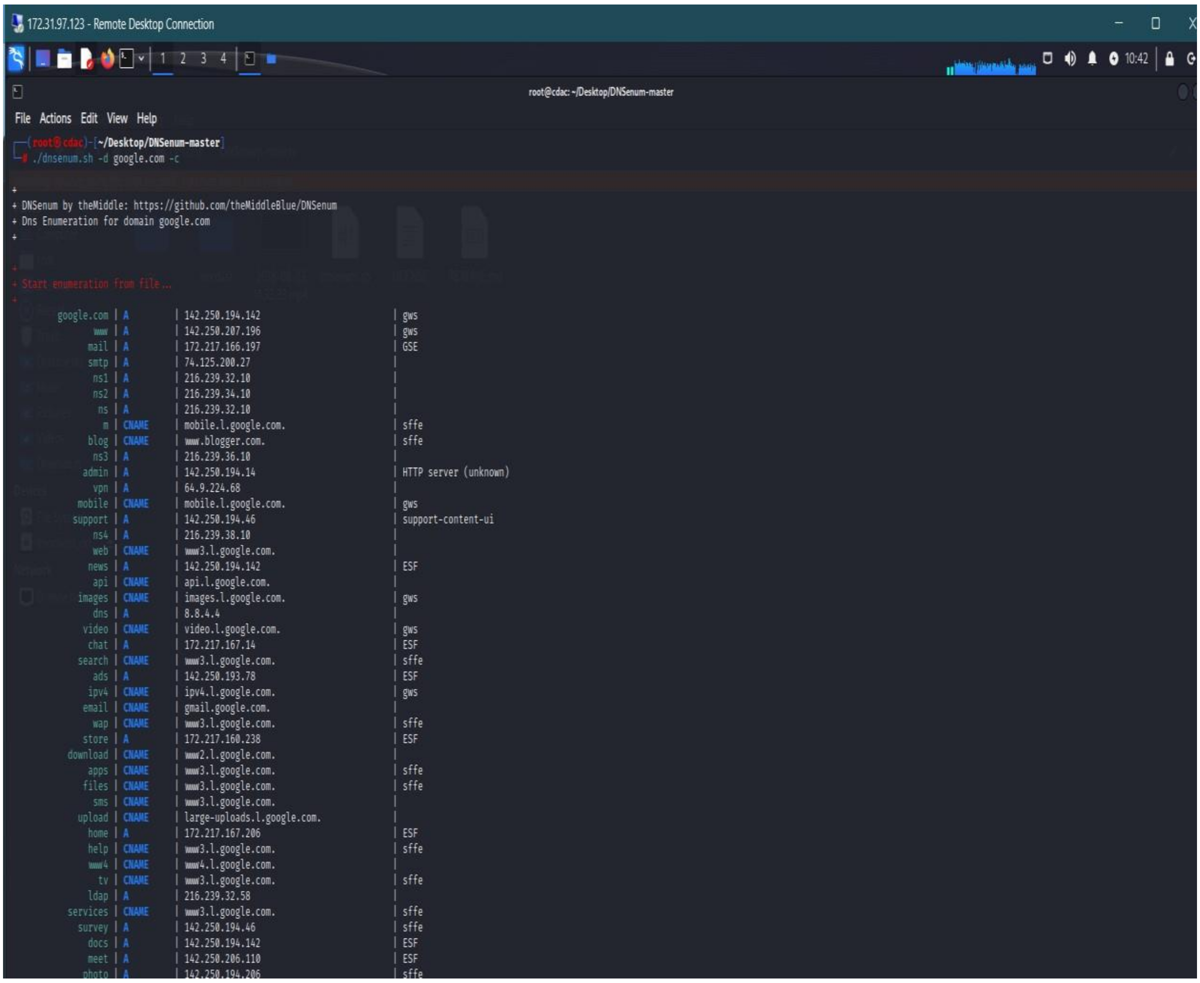
<u>DNS ENUM</u>

<u>Name-> Vijay Bhushan Singh</u>
<u>E-mail-> vijay8303blw@gmail.com</u>
<u>College-> Indian Institute of Information Technology, Manipur</u>
<u>Phone_no-> 8303420912</u>

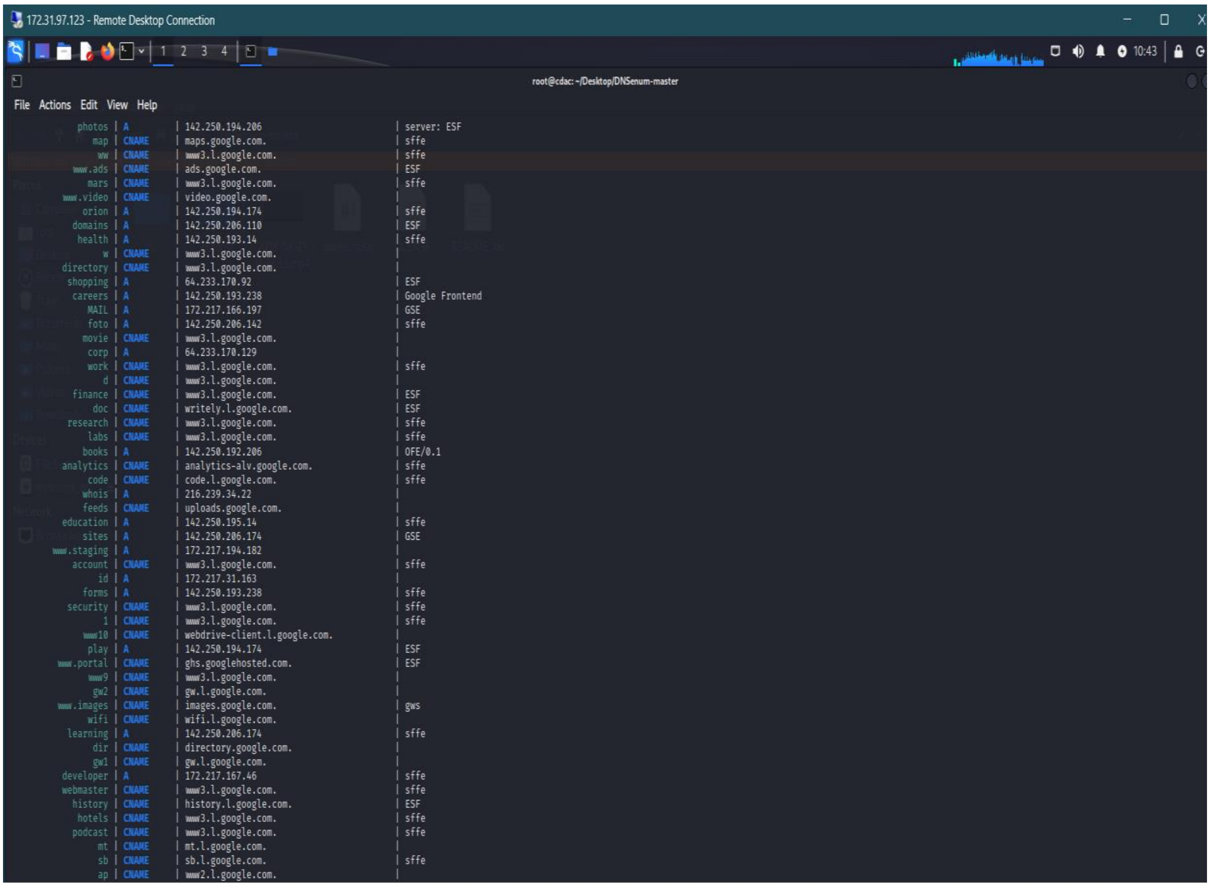
Simply running the command to get all the sub-domains under that domain.

i.e. <u>/dnsenum.sh -d google.com -c</u>

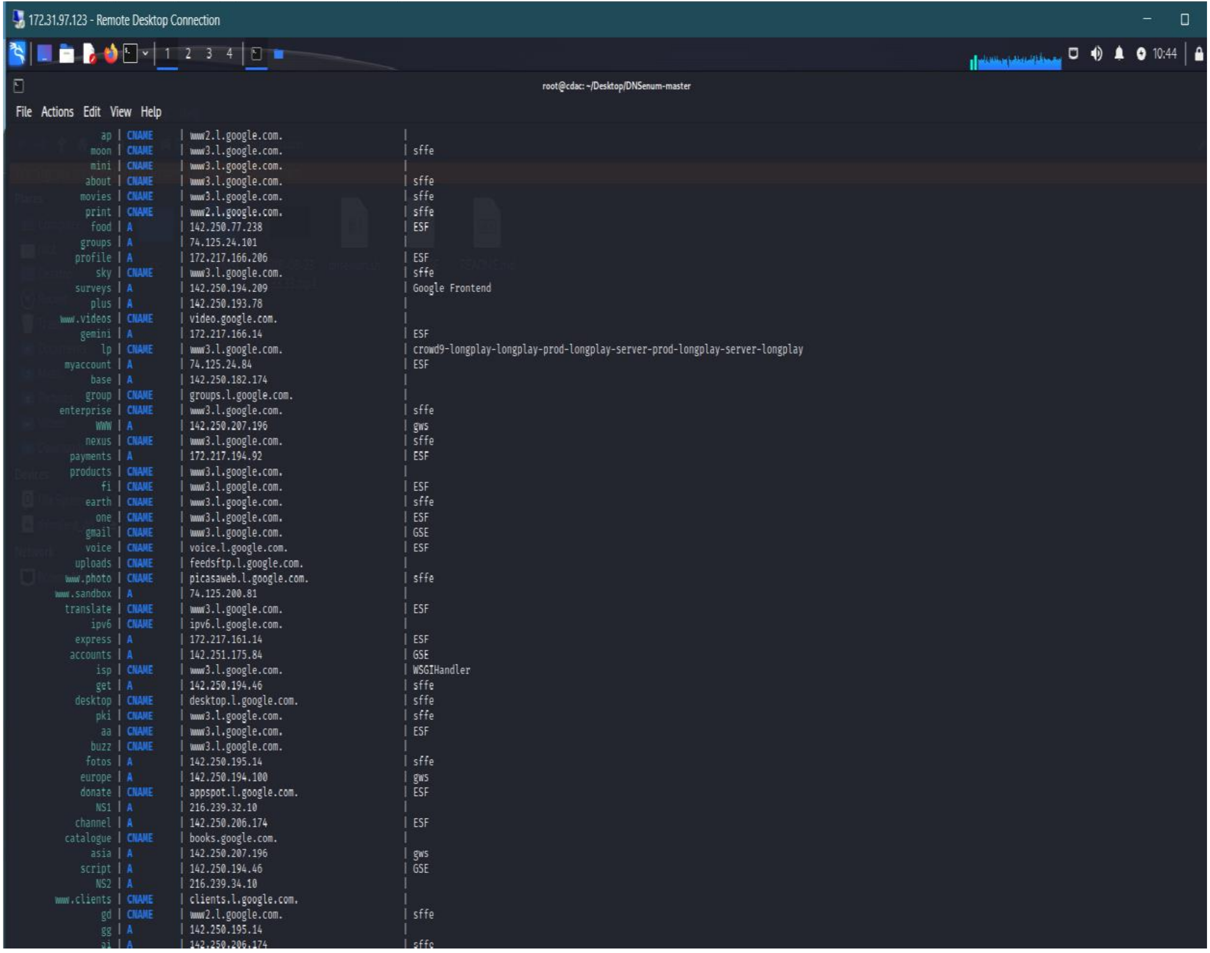


172.31.97.123 - Remote Desktop Connection
1 2 3 4
10:42
root@cdac: ~/Desktop/DNSenum-master
File Actions Edit View Help

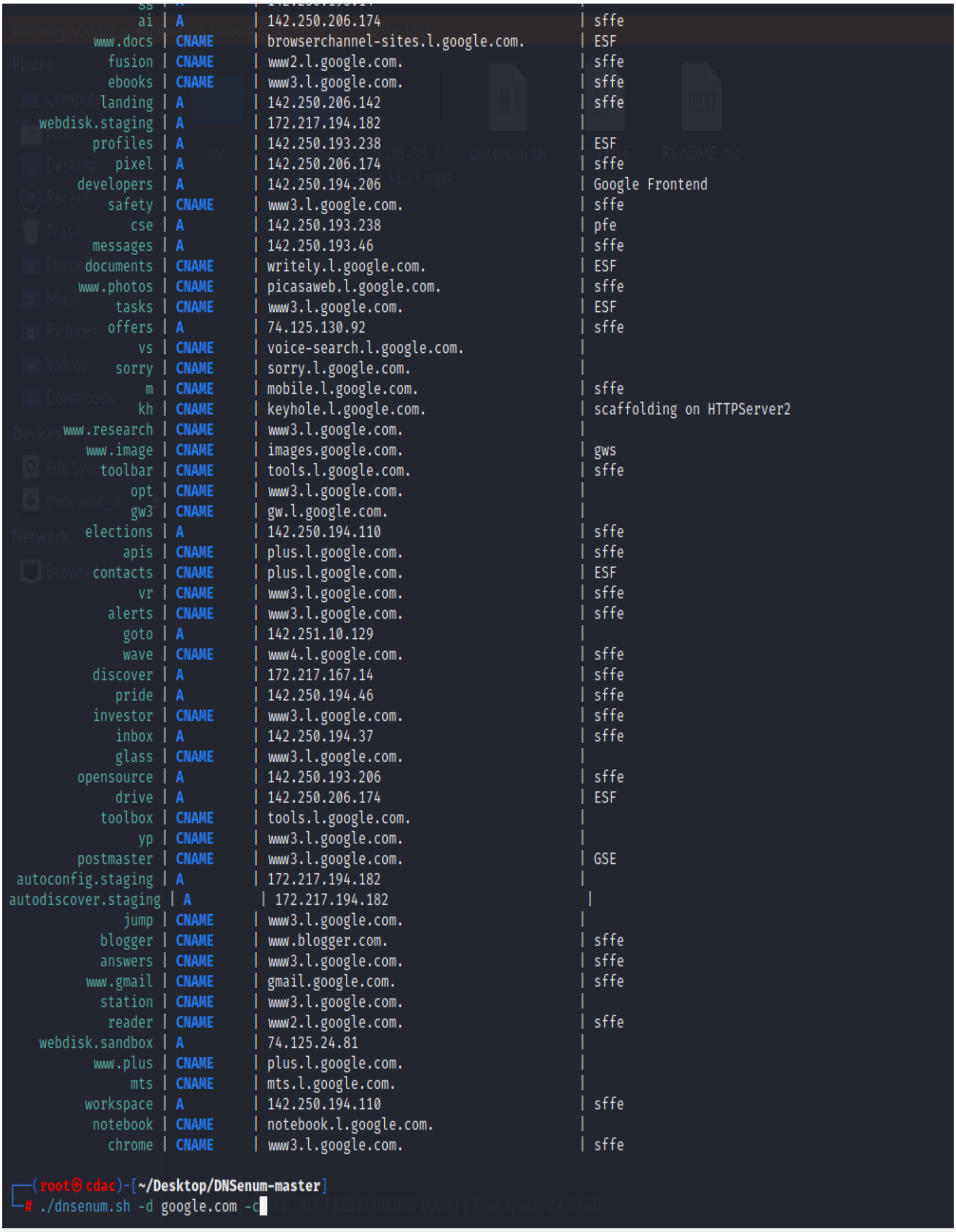
```
┌──(root㉿cdac)-[~/Desktop/DNSenum-master]
└─# ./dnsenum.sh -d google.com -c

+
+ DNSenum by theMiddle: https://github.com/theMiddleBlue/DNSenum
+ Dns Enumeration for domain google.com
+

+
+ Start enumeration from file...
+
    google.com | A       | 142.250.194.142                   | gws
           www | A       | 142.250.207.196                   | gws
          mail | A       | 172.217.166.197                   | GSE
          smtp | A       | 74.125.200.27                     |
           ns1 | A       | 216.239.32.10                     |
           ns2 | A       | 216.239.34.10                     |
            ns | A       | 216.239.32.10                     |
             m | CNAME   | mobile.l.google.com.              | sffe
          blog | CNAME   | www.blogger.com.                  | sffe
           ns3 | A       | 216.239.36.10                     |
         admin | A       | 142.250.194.14                    | HTTP server (unknown)
           vpn | A       | 64.9.224.68                       |
        mobile | CNAME   | mobile.l.google.com.              | gws
       support | A       | 142.250.194.46                    | support-content-ui
           ns4 | A       | 216.239.38.10                     |
           web | CNAME   | www3.l.google.com.                |
          news | A       | 142.250.194.142                   | ESF
           api | CNAME   | api.l.google.com.                 |
        images | CNAME   | images.l.google.com.              | gws
           dns | A       | 8.8.4.4                           |
         video | CNAME   | video.l.google.com.               | gws
          chat | A       | 172.217.167.14                    | ESF
        search | CNAME   | www3.l.google.com.                | sffe
           ads | A       | 142.250.193.78                    | ESF
          ipv4 | CNAME   | ipv4.l.google.com.                | gws
         email | CNAME   | gmail.google.com.                 |
           wap | CNAME   | www3.l.google.com.                | sffe
         store | A       | 172.217.160.238                   | ESF
      download | CNAME   | www2.l.google.com.                |
          apps | CNAME   | www3.l.google.com.                | sffe
         files | CNAME   | www3.l.google.com.                | sffe
           sms | CNAME   | www3.l.google.com.                |
        upload | CNAME   | large-uploads.l.google.com.       |
          home | A       | 172.217.167.206                   | ESF
          help | CNAME   | www3.l.google.com.                | sffe
          www4 | CNAME   | www4.l.google.com.                |
            tv | CNAME   | www3.l.google.com.                | sffe
          ldap | A       | 216.239.32.58                     |
      services | CNAME   | www3.l.google.com.                | sffe
        survey | A       | 142.250.194.46                    | sffe
          docs | A       | 142.250.194.142                   | ESF
          meet | A       | 142.250.206.110                   | ESF
         photo | A       | 142.250.194.206                   | sffe
```


172.31.97.123 - Remote Desktop Connection
1 2 3 4
10:43
root@cdac: ~/Desktop/DNSenum-master
File Actions Edit View Help

```
     photos | A     | 142.250.194.206                  | server: ESF
        map | CNAME | maps.google.com.                 | sffe
         ww | CNAME | www3.l.google.com.               | sffe
    www.ads | CNAME | ads.google.com.                  | ESF
       mars | CNAME | www3.l.google.com.               | sffe
  www.video | CNAME | video.google.com.                |
      orion | A     | 142.250.194.174                  | sffe
    domains | A     | 142.250.206.110                  | ESF
     health | A     | 142.250.193.14                   | sffe
          w | CNAME | www3.l.google.com.               |
  directory | CNAME | www3.l.google.com.               |
   shopping | A     | 64.233.170.92                    | ESF
    careers | A     | 142.250.193.238                  | Google Frontend
       MAIL | A     | 172.217.166.197                  | GSE
       foto | A     | 142.250.206.142                  | sffe
      movie | CNAME | www3.l.google.com.               |
       corp | A     | 64.233.170.129                   |
       work | CNAME | www3.l.google.com.               | sffe
          d | CNAME | www3.l.google.com.               |
    finance | CNAME | www3.l.google.com.               | ESF
        doc | CNAME | writely.l.google.com.            | ESF
   research | CNAME | www3.l.google.com.               | sffe
       labs | CNAME | www3.l.google.com.               | sffe
      books | A     | 142.250.192.206                  | OFE/0.1
  analytics | CNAME | analytics-alv.google.com.        | sffe
       code | CNAME | code.l.google.com.               | sffe
      whois | A     | 216.239.34.22                    |
      feeds | CNAME | uploads.google.com.              |
  education | A     | 142.250.195.14                   | sffe
      sites | A     | 142.250.206.174                  | GSE
www.staging | A     | 172.217.194.182                  |
    account | CNAME | www3.l.google.com.               | sffe
         id | A     | 172.217.31.163                   |
      forms | A     | 142.250.193.238                  | sffe
   security | CNAME | www3.l.google.com.               | sffe
          1 | CNAME | www3.l.google.com.               | sffe
      www10 | CNAME | webdrive-client.l.google.com.    |
       play | A     | 142.250.194.174                  | ESF
 www.portal | CNAME | ghs.googlehosted.com.            | ESF
       www9 | CNAME | www3.l.google.com.               |
        gw2 | CNAME | gw.l.google.com.                 |
 www.images | CNAME | images.google.com.               | gws
       wifi | CNAME | wifi.l.google.com.               |
   learning | A     | 142.250.206.174                  | sffe
        dir | CNAME | directory.google.com.            |
        gw1 | CNAME | gw.l.google.com.                 |
  developer | A     | 172.217.167.46                   | sffe
  webmaster | CNAME | www3.l.google.com.               | sffe
    history | CNAME | history.l.google.com.            | ESF
     hotels | CNAME | www3.l.google.com.               | sffe
    podcast | CNAME | www3.l.google.com.               | sffe
         mt | CNAME | mt.l.google.com.                 |
         sb | CNAME | sb.l.google.com.                 | sffe
         ap | CNAME | www2.l.google.com.               |
```


172.31.97.123 - Remote Desktop Connection
1 2 3 4
10:44
root@cdac: ~/Desktop/DNSenum-master
File Actions Edit View Help

```
         ap | CNAME | www2.l.google.com.               |
       moon | CNAME | www3.l.google.com.               | sffe
       mini | CNAME | www3.l.google.com.               |
      about | CNAME | www3.l.google.com.               | sffe
     movies | CNAME | www3.l.google.com.               | sffe
      print | CNAME | www2.l.google.com.               | sffe
       food | A     | 142.250.77.238                   | ESF
     groups | A     | 74.125.24.101                    |
    profile | A     | 172.217.166.206                  | ESF
        sky | CNAME | www3.l.google.com.               | sffe
    surveys | A     | 142.250.194.209                  | Google Frontend
       plus | A     | 142.250.193.78                   |
 www.videos | CNAME | video.google.com.                |
     gemini | A     | 172.217.166.14                   | ESF
         lp | CNAME | www3.l.google.com.               | crowd9-longplay-longplay-prod-longplay-server-prod-longplay-server-longplay
  myaccount | A     | 74.125.24.84                     | ESF
       base | A     | 142.250.182.174                  |
      group | CNAME | groups.l.google.com.             |
 enterprise | CNAME | www3.l.google.com.               | sffe
        WWW | A     | 142.250.207.196                  | gws
      nexus | CNAME | www3.l.google.com.               | sffe
   payments | A     | 172.217.194.92                   | ESF
   products | CNAME | www3.l.google.com.               |
         fi | CNAME | www3.l.google.com.               | ESF
      earth | CNAME | www3.l.google.com.               | sffe
        one | CNAME | www3.l.google.com.               | ESF
      gmail | CNAME | www3.l.google.com.               | GSE
      voice | CNAME | voice.l.google.com.              | ESF
    uploads | CNAME | feedsftp.l.google.com.           |
  www.photo | CNAME | picasaweb.l.google.com.          | sffe
www.sandbox | A     | 74.125.200.81                    |
  translate | CNAME | www3.l.google.com.               | ESF
       ipv6 | CNAME | ipv6.l.google.com.               |
    express | A     | 172.217.161.14                   | ESF
   accounts | A     | 142.251.175.84                   | GSE
        isp | CNAME | www3.l.google.com.               | WSGIHandler
        get | A     | 142.250.194.46                   | sffe
    desktop | CNAME | desktop.l.google.com.            | sffe
        pki | CNAME | www3.l.google.com.               | sffe
         aa | CNAME | www3.l.google.com.               | ESF
       buzz | CNAME | www3.l.google.com.               |
      fotos | A     | 142.250.195.14                   | sffe
     europe | A     | 142.250.194.100                  | gws
     donate | CNAME | appspot.l.google.com.            | ESF
        NS1 | A     | 216.239.32.10                    |
    channel | A     | 142.250.206.174                  | ESF
  catalogue | CNAME | books.google.com.                |
       asia | A     | 142.250.207.196                  | gws
     script | A     | 142.250.194.46                   | GSE
        NS2 | A     | 216.239.34.10                    |
www.clients | CNAME | clients.l.google.com.            |
         gd | CNAME | www2.l.google.com.               | sffe
         gg | A     | 142.250.195.14                   |
         ai | A     | 142.250.206.174                  | sffe
```



```
                 ai | A       | 142.250.206.174                        | sffe
           www.docs | CNAME   | browserchannel-sites.l.google.com.     | ESF
             fusion | CNAME   | www2.l.google.com.                     | sffe
             ebooks | CNAME   | www3.l.google.com.                     | sffe
            landing | A       | 142.250.206.142                        | sffe
     webdisk.staging | A      | 172.217.194.182                        |
           profiles | A       | 142.250.193.238                        | ESF
              pixel | A       | 142.250.206.174                        | sffe
         developers | A       | 142.250.194.206                        | Google Frontend
             safety | CNAME   | www3.l.google.com.                     | sffe
                cse | A       | 142.250.193.238                        | pfe
           messages | A       | 142.250.193.46                         | sffe
          documents | CNAME   | writely.l.google.com.                  | ESF
         www.photos | CNAME   | picasaweb.l.google.com.                | sffe
              tasks | CNAME   | www3.l.google.com.                     | ESF
             offers | A       | 74.125.130.92                          | sffe
                 vs | CNAME   | voice-search.l.google.com.             |
              sorry | CNAME   | sorry.l.google.com.                    |
                  m | CNAME   | mobile.l.google.com.                   | sffe
                 kh | CNAME   | keyhole.l.google.com.                  | scaffolding on HTTPServer2
       www.research | CNAME   | www3.l.google.com.                     |
          www.image | CNAME   | images.google.com.                     | gws
            toolbar | CNAME   | tools.l.google.com.                    | sffe
                opt | CNAME   | www3.l.google.com.                     |
                gw3 | CNAME   | gw.l.google.com.                       |
          elections | A       | 142.250.194.110                        | sffe
               apis | CNAME   | plus.l.google.com.                     | sffe
           contacts | CNAME   | plus.l.google.com.                     | ESF
                 vr | CNAME   | www3.l.google.com.                     | sffe
             alerts | CNAME   | www3.l.google.com.                     | sffe
               goto | A       | 142.251.10.129                         |
               wave | CNAME   | www4.l.google.com.                     | sffe
           discover | A       | 172.217.167.14                         | sffe
              pride | A       | 142.250.194.46                         | sffe
           investor | CNAME   | www3.l.google.com.                     | sffe
              inbox | A       | 142.250.194.37                         | sffe
              glass | CNAME   | www3.l.google.com.                     |
         opensource | A       | 142.250.193.206                        | sffe
              drive | A       | 142.250.206.174                        | ESF
            toolbox | CNAME   | tools.l.google.com.                    |
                 yp | CNAME   | www3.l.google.com.                     |
         postmaster | CNAME   | www3.l.google.com.                     | GSE
  autoconfig.staging | A      | 172.217.194.182                        |
autodiscover.staging | A       | 172.217.194.182                        |
               jump | CNAME   | www3.l.google.com.                     |
            blogger | CNAME   | www.blogger.com.                       | sffe
            answers | CNAME   | www3.l.google.com.                     | sffe
          www.gmail | CNAME   | gmail.google.com.                      | sffe
            station | CNAME   | www3.l.google.com.                     |
             reader | CNAME   | www2.l.google.com.                     | sffe
     webdisk.sandbox | A      | 74.125.24.81                           |
           www.plus | CNAME   | plus.l.google.com.                     |
                mts | CNAME   | mts.l.google.com.                      |
          workspace | A       | 142.250.194.110                        | sffe
           notebook | CNAME   | notebook.l.google.com.                 |
             chrome | CNAME   | www3.l.google.com.                     | sffe

┌──(root㉿cdac)-[~/Desktop/DNSenum-master]
└─# ./dnsenum.sh -d google.com -c
```

Hence it has given everything about this domain present in server.
