Reconnaissance Report

Index

Reconnaissance Report

This report contains various analyses of the provided URL.

The tools used.

IPWhois: For obtaining geolocation and hosting information.

sublist3r: For enumerating subdomains.

whois: For getting WHOIS information.

nmap: For scanning ports.

domain

google.com

ip

142.250.70.46

ipinfo

```
{
  "ip": "142.250.70.46",
  "hostname": "pnbomb-aa-in-f14.1e100.net",
  "city": "Mumbai",
  "region": "Maharashtra",
  "country": "IN",
  "loc": "19.0728,72.8826",
  "org": "AS15169 Google LLC",
  "postal": "400017",
  "timezone": "Asia/Kolkata"
}
```

NMap

Host: 142.250.70.46 (google.com)

State: up

Protocol: tcp

Port: 80, State: open

Port: 443, State: open

whois

domain_name: GOOGLE.COM

registrar: MarkMonitor, Inc.

registrar_url: http://www.markmonitor.com

reseller: None

whois_server: whois.markmonitor.com

referral_url: None

updated_date: [datetime.datetime(2019, 9, 9, 15, 39, 4), datetime.datetime(2024, 8, 2, 2, 17, 33, tzinfo=datetime.timezone.utc)]

creation_date: [datetime.datetime(1997, 9, 15, 4, 0), datetime.datetime(1997, 9, 15, 7, 0, tzinfo=datetime.timezone.utc)]

expiration_date: [datetime.datetime(2028, 9, 14, 4, 0), datetime.datetime(2028, 9, 13, 7, 0, tzinfo=datetime.timezone.utc)]

name_servers: ['NS1.GOOGLE.COM', 'NS2.GOOGLE.COM', 'NS3.GOOGLE.COM', 'NS4.GOOGLE.COM']

status: ['clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited', 'clientTransferProhibited https://icann.org/epp#clientTransferProhibited', 'clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited', 'serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited', 'serverTransferProhibited https://icann.org/epp#serverTransferProhibited', 'serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited', 'clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)', 'clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)', 'clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)', 'serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)', 'serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)', 'serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)']

emails: ['abusecomplaints@markmonitor.com', 'whoisrequest@markmonitor.com']

dnssec: unsigned

name: None

org: Google LLC

address: None

city: None

state: CA

registrant_postal_code: None

country: US

DNS

A Records: ['142.250.70.46']

MX Records: ['10 smtp.google.com.']

NS Records: ['ns2.google.com.', 'ns1.google.com.', 'ns4.google.com.', 'ns3.google.com.']

TXT Records (Text): ['"v=spf1 include:_spf.google.com ~all"', '"cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"', '"google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"', '"docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"', '"docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"', '"onetrust-domain-verification=de01ed21f2fa4d8781cbc3ffb89cf4ef"', '"MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"', '"apple-domain-verification=30afIBcvSuDV2PLX"', '"google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"', '"globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="', '"facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"', '"google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"']

CNAME Record (Alias): ['No CNAME Record found.']

SOA Record (Authority): ['ns1.google.com. dns-admin.google.com. 705439661 900 900 1800 60']

Trace Route

```
 1  192.168.0.1 (192.168.0.1)  6.051 ms  3.832 ms  3.832 ms

 2  * * *

 3  56.14.206.193 (56.14.206.193)  84.948 ms

    56.14.206.173 (56.14.206.173)  74.453 ms

    56.14.206.177 (56.14.206.177)  73.963 ms

 4  172.27.249.4 (172.27.249.4)  50.164 ms  73.317 ms  48.283 ms

 5  172.27.249.35 (172.27.249.35)  77.210 ms  65.215 ms  64.679 ms

 6  192.168.239.6 (192.168.239.6)  55.086 ms

    192.168.239.10 (192.168.239.10)  60.512 ms

    192.168.239.12 (192.168.239.12)  69.918 ms

 7  * * *

 8  * * *

 9  * * *

10  * * *

11  * * *

12  49.44.18.38 (49.44.18.38)  91.315 ms * *

13  * * *

14  * * *

15  * * *

16  142.250.239.170 (142.250.239.170)  97.905 ms

    192.178.110.204 (192.178.110.204)  115.149 ms
    192.178.86.238 (192.178.86.238)  86.772 ms
17  192.178.86.245 (192.178.86.245)  75.340 ms
    142.250.209.71 (142.250.209.71)  89.780 ms
    192.178.111.61 (192.178.111.61)  82.436 ms
18  pnbomb-aa-in-f14.1e100.net (142.250.70.46)  83.773 ms  79.590 ms
    142.251.77.69 (142.251.77.69)  91.066 ms
```

Subdomain

*.apis.corp.google.com

*.appengine.google.com

*.auth.corp.google.com

*.bigstore-test.corp.google.com

*.bigstore.corp.google.com

*.blogger.corp.google.com

*.blogspot.corp.google.com

*.c.docs.google.com

*.c.pack.google.com

*.c.play.google.com

*.c.video.google.com

*.cache1.c.docs.google.com

*.cache1.c.play.google.com

*.cache1.c.video.google.com

*.cache2.c.docs.google.com

*.cache2.c.play.google.com

*.cache2.c.video.google.com

*.cache3.c.docs.google.com

*.cache3.c.play.google.com

*.cache3.c.video.google.com

*.cache4.c.docs.google.com

*.cache4.c.play.google.com

*.cache4.c.video.google.com

*.cache5.c.docs.google.com

*.cache5.c.play.google.com

*.cache5.c.video.google.com

*.cache6.c.docs.google.com

*.cache6.c.play.google.com

*.cache6.c.video.google.com

*.cache7.c.docs.google.com

*.cache7.c.play.google.com

*.cache7.c.video.google.com

*.cache8.c.docs.google.com

*.cache8.c.play.google.com

*.cache8.c.video.google.com

*.cag.ext.google.com

*.chrome.google.com

*.client-channel.google.com

*.clients.google.com

*.cloud.google.com

*.code.google.com

*.corp-backups.corp.google.com

*.corp.google.com

*.dasher-qa.corp.google.com

*.dasher.corp.google.com

*.demetrius-codespot.corp.google.com

*.demetrius-googlecode.corp.google.com

*.demetrius.corp.google.com

*.devconsole-testers.sandbox.google.com

*.developer.google.com

*.developers.google.com

*.dfa7.corp.google.com

*.docs-dev.corp.google.com

*.docs-nightly.corp.google.com

*.docs-platinum.corp.google.com

*.docs-qa.corp.google.com

*.docs.google.com

*.docs.sandbox.google.com

*.drive-test.corp.google.com

*.drive.google.com

*.drive.sandbox.google.com

*.dthree.corp.google.com

*.ext.google.com

*.focus.corp.google.com

*.friendconnect.google.com

*.games.corp.google.com

*.git.corp.google.com

*.glass.ext.google.com

*.google.com

*.google.com.af

*.google.com.ag

*.google.com.ai

*.google.com.ar

*.google.com.au

*.google.com.bd

*.google.com.bh

*.google.com.bn

*.google.com.bo

*.google.com.br

*.google.com.by

*.google.com.bz

*.google.com.cn

*.google.com.co

*.google.com.cu

*.google.com.cy

*.google.com.do

*.google.com.ec

*.google.com.eg

*.google.com.et

*.google.com.fj

*.google.com.ge

*.google.com.gh

*.google.com.gi

*.google.com.gr

*.google.com.gt

*.google.com.hk

*.google.com.iq

*.google.com.jm

*.google.com.jo

*.google.com.kh

*.google.com.kw

*.google.com.lb

*.google.com.ly

*.google.com.mm

*.google.com.mt

*.google.com.mx

*.google.com.my

*.google.com.na

*.google.com.nf

*.google.com.ng

*.google.com.ni

*.google.com.np

*.google.com.nr

*.google.com.om

*.google.com.pa

*.google.com.pe

*.google.com.pg

*.google.com.ph

*.google.com.pk

*.google.com.pl

*.google.com.pr

*.google.com.py

*.google.com.qa

*.google.com.ru

*.google.com.sa

*.google.com.sb

*.google.com.sg

*.google.com.sl

*.google.com.sv

*.google.com.tj

*.google.com.tn

*.google.com.tr

*.google.com.tw

*.google.com.ua

*.google.com.uy

*.google.com.vc

*.google.com.ve

*.google.com.vn

*.googlesource.corp.google.com

*.ice.ext.google.com

*.jotspot-qa08.corp.google.com

*.loop.corp.google.com

*.mail.google.com

*.meeting.ext.google.com

*.orkut-fixprod.corp.google.com

*.orkut-impersonation.corp.google.com

*.orkut-ocdemo.corp.google.com

*.orkut-qa.corp.google.com

*.orkut-staging.corp.google.com

*.orkut-uberproxy.corp.google.com

*.orkut-vctask0.corp.google.com

*.orkut-vcvrfy.corp.google.com

*.orkut-yhtask0.corp.google.com

*.orkut-yhvrfy.corp.google.com

*.orkut-yqtask0.corp.google.com

*.orkut-yqvrfy.corp.google.com

*.oz-gmail.corp.google.com

*.oz-s2.corp.google.com

*.oz-www.corp.google.com

*.photos.google.com

*.plus.corp.google.com

*.plus.google.com

*.plusone.corp.google.com

*.postini.corp.google.com

*.profiles.corp.google.com

*.prom-qa.corp.google.com

*.prom-qa.sandbox.google.com

*.prom-test.corp.google.com

*.prom-test.sandbox.google.com

*.prom.corp.google.com

*.qa.adz.google.com

*.sandbox.google.com

*.sandbox.google.com.au

*.sandbox.google.com.br

*.sandbox.google.com.hk

*.script.sandbox.google.com

*.search.corp.google.com

*.sites-googlegroups-nightly.corp.google.com

*.sites-googlegroups-qa01.corp.google.com

*.sites-googlegroups-qa02.corp.google.com

*.sites-googlegroups-qa03.corp.google.com

*.sites-googlegroups-qa04.corp.google.com

*.sites-googlegroups-qa05.corp.google.com

*.sites-googlegroups-qa06.corp.google.com

*.sites-googlegroups-qa07.corp.google.com

*.sites-googlegroups-qa08.corp.google.com

*.sites-googlegroups-tctest.corp.google.com

*.sites.google.com

*.sites.sandbox.google.com

*.spdy-proxy.ext.google.com

*.staging-a.blogger.corp.google.com

*.staging-b.blogger.corp.google.com

*.staging-c.blogger.corp.google.com

*.staging-d.blogger.corp.google.com

*.staging-daily.blogger.corp.google.com

*.staging-daily.blogspot.corp.google.com

*.staging-gaia.blogger.corp.google.com

*.staging-git.corp.google.com

*.staging-googlesource.corp.google.com

*.staging-prod.blogger.corp.google.com

*.staging-weekly.blogger.corp.google.com

*.staging-weekly.blogspot.corp.google.com

*.talkgadget.google.com

*.test.postini.corp.google.com

*.upload.google.com

*.urchin.corp.google.com

*.url.google.com

*.vp.video.l.google.com

*.webdrive-test-canary.corp.google.com

*.webdrive-test-prod.corp.google.com

aarjav-b480g7k2ab9@checkout.google.com

accounts.flexpack.google.com

accounts.freezone.google.com

accounts.google.com

admin@google.com

ads-compare.eem.corp.google.com

adwords.google.com

adwords.google.com.ar

adwords.google.com.au

adwords.google.com.br

adwords.google.com.cn

adwords.google.com.gr

adwords.google.com.hk

adwords.google.com.ly

adwords.google.com.mx

adwords.google.com.my

adwords.google.com.pe

adwords.google.com.ph

adwords.google.com.pk

adwords.google.com.ru

adwords.google.com.sg

adwords.google.com.tr

adwords.google.com.tw

adwords.google.com.ua

adwords.google.com.vn

alt1.aspmx.l.google.com

alt1.gmail-smtp-in.l.google.com

alt1.gmr-smtp-in.l.google.com

alt2.aspmx.l.google.com

alt2.gmail-smtp-in.l.google.com

alt2.gmr-smtp-in.l.google.com

alt3.aspmx.l.google.com

alt3.gmail-smtp-in.l.google.com

alt3.gmr-smtp-in.l.google.com

alt4.aspmx.l.google.com

alt4.gmail-smtp-in.l.google.com

alt4.gmr-smtp-in.l.google.com

answers.google.com

apps-secure-data-connector.google.com

aspmx.l.google.com

audioads.google.com

bmcquade@google.com

cag.ext.google.com

cert-test.sandbox.google.com

checkout.google.com

cod.ext.google.com

da.ext.corp.google.com

da.ext.google.com

dg.video.google.com

ecc-test.sandbox.google.com

eggroll.ext.google.com

ext.google.com

flexpack.google.com

fra-da.ext.google.com

freezone.accounts.google.com

freezone.google.com

freezone.m.google.com

freezone.mail.google.com

gaiastaging.flexpack.google.com

gaiastaging.freezone.google.com

glass-eur.ext.google.com

glass-mtv.ext.google.com

glass-twd.ext.google.com

glass.ext.google.com

gmail-smtp-in.l.google.com

gmail.google.com

gmr-smtp-in.l.google.com

google.com

google.com.af

google.com.ag

google.com.ai

google.com.ar

google.com.au

google.com.bd

google.com.bh

google.com.bn

google.com.bo

google.com.br

google.com.by

google.com.bz

google.com.cn

google.com.co

google.com.cu

google.com.cy

google.com.do

google.com.ec

google.com.eg

google.com.et

google.com.fj

google.com.ge

google.com.gh

google.com.gi

google.com.gr

google.com.gt

google.com.hk

google.com.iq

google.com.jm

google.com.jo

google.com.kh

google.com.kw

google.com.lb

google.com.ly

google.com.mm

google.com.mt

google.com.mx

google.com.my

google.com.na

google.com.nf

google.com.ng

google.com.ni

google.com.np

google.com.nr

google.com.om

google.com.pa

google.com.pe

google.com.pg

google.com.ph

google.com.pk

google.com.pl

google.com.pr

google.com.py

google.com.qa

google.com.ru

google.com.sa

google.com.sb

google.com.sg

google.com.sl

google.com.sv

google.com.tj

google.com.tn

google.com.tr

google.com.tw

google.com.ua

google.com.uy

google.com.vc

google.com.ve

google.com.vn

hosted-id.google.com

hot-da.ext.google.com

hyd-da.ext.google.com

ice.ext.google.com

ics.prod.google.com

jmt0.google.com

login.corp.google.com

m.google.com

m.guts.corp.google.com

m.gutsdev.corp.google.com

mail.flexpack.google.com

mail.freezone.google.com

mail.google.com

meeting.ext.google.com

misc-sni.google.com

misc.google.com

mtalk.google.com

mtv-da-1.ad.corp.google.com

mtv-da.corp.google.com

mtv-da.ext.google.com

mx.google.com

mygeist.corp.google.com

mygeist2010.corp.google.com

news.freezone.google.com

onex.wifi.google.com

plus.flexpack.google.com

plus.freezone.google.com

proxyconfig.corp.google.com

qa.adz.google.com

reseed.corp.google.com

sandbox.google.com

search.flexpack.google.com

search.freezone.google.com

services.google.com

soaproxyprod01.ext.google.com

soaproxytest01.ext.google.com

spdy-proxy-debug.ext.google.com

spdy-proxy.ext.google.com

talk.google.com

twd-da.ext.google.com

twdsalesgsa.twd.corp.google.com

uberproxy-nocert.corp.google.com

uberproxy-san.corp.google.com

uberproxy.corp.google.com

upload.google.com

upload.video.google.com

vp.video.l.google.com

wifi.google.com

www.flexpack.google.com

www.freezone.google.com

www.google.com

www.google.com\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232\341\205\232.phreedom.org