
metadata

Metadata

```
~ scamper -v
scamper version 20240813
```

```
~ sudo scamper -I "tracelb 8.8.8.8"
tracelb from 192.168.1.129 to 8.8.8.8, 3 nodes, 2 links, 56 probes, 95%
192.168.1.1 -> 190.20.192.1
190.20.192.1 -> (10.50.3.9, *) -> (10.50.3.10, *) -> (192.178.68.148, 72.14.202.154, 72.14.243.170) -> * -> 8.8.8.8
```

```
~ dig -x 190.20.192.1 | grep PTR
;1.192.20.190.in-addr.arpa.     IN      PTR
1.192.20.190.in-addr.arpa. 6347 IN      PTR     190-20-192-1.baf.movistar.cl.
~ dig +short 1.192.20.190.origin.asn.cymru.com TXT
"7418 | 190.20.0.0/16 | CL | lacnic | 2006-06-12"
```

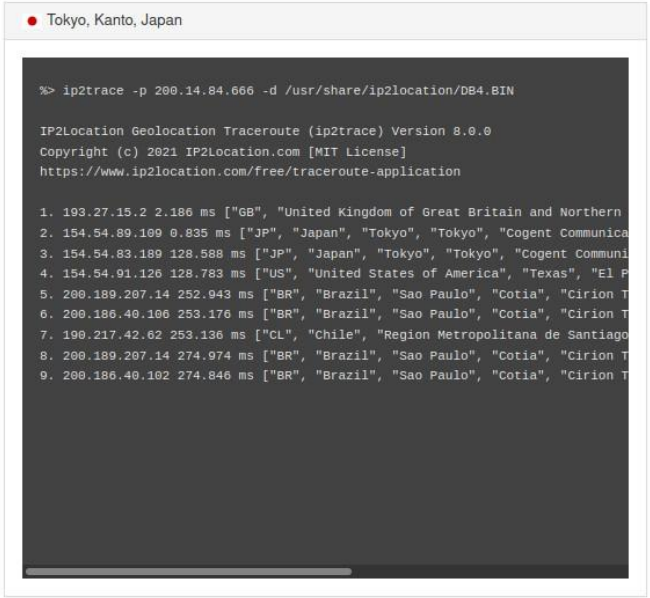
Geolocation

Business


```
{
  "ip": "190.20.197.159",
  "hostname": "190-20-197-1
  "city": "Santiago",
  "region": "Santiago Metro
  "country": "CL",
  "loc": "-33.4569,-70.6483
  "postal": "8320000",
  "timezone": "America/Sant
  "asn": {
    "asn": "AS7418",
    "name": "TELEFÓNICA CHI
    "domain": "telefonicach
    "route": "190.20.0.0/16
    "type": "isp"
  },
  "company": {
    "name": "TELEFÓNICA CHI
    "domain": "telefonicade
    "type": "isp"
  },
  "privacy": {
    "vpn": false,
    "proxy": false,
    "tor": false,
    "relay": false,
    "hosting": false,
    "service": ""
  },
  "abuse": {
    "address": "Providencia
    "country": "CL",
    "email": "tecnical.isp.
    "name": "Technical Cont
    "network": "190.20.0.0/
    "phone": "+56  26616815
  },
```

IP2Trace

pip install IP2Trace




```
cursos/ruteo/sample.bin.db4 sudo ip2tracepy -p 193.27.15.2 -d IP-COUNTRY
-REGION-CITY-ISP-SAMPLE.BIN
IP2Location Geolocation Traceroute (ip2trace) Version 3.2.0
Copyright (c) 2022 IP2Location.com [MIT License]
https://www.ip2location.com/free/traceroute-application


Traceroute to 193.27.15.2

 1  192.168.31.1  0.527ms 0.467ms 0.592ms ["-","This is IP2Location DB4 IPv4 sa
mple BIN database. Please evaluate IP address from 0.0.0.0 to 99.255.255.255.",
"This is IP2Location DB4 IPv4 sample BIN database. Please evaluate IP address f
rom 0.0.0.0 to 99.255.255.255."]
 2  200.14.84.9  1.240ms 1.265ms 1.253ms ["-","This is IP2Location DB4 IPv4 sam
ple BIN database. Please evaluate IP address from 0.0.0.0 to 99.255.255.255.","
This is IP2Location DB4 IPv4 sample BIN database. Please evaluate IP address fr
om 0.0.0.0 to 99.255.255.255."]
```

```
cursos/ruteo/sample.bin.db4 sudo ip2tracepy -p 193.27.15.2
IP2Location Geolocation Traceroute (ip2trace) Version 3.2.0
Copyright (c) 2022 IP2Location.com [MIT License]
https://www.ip2location.com/free/traceroute-application


Traceroute to 193.27.15.2

 1  192.168.31.1  0.579ms 0.687ms 0.545ms ["-"]
 2  200.14.84.9  1.189ms 0.959ms 1.138ms ["CL"]
 3  192.168.0.89  1.443ms 1.348ms 1.370ms ["-"]
 4  172.19.0.249  1.190ms 1.175ms 1.168ms ["-"]
 5  190.217.42.249  7.292ms 7.339ms 7.833ms ["CL"]
 6  *
 7  *
 8  *
 9  *
10  *
```

IP to GPS

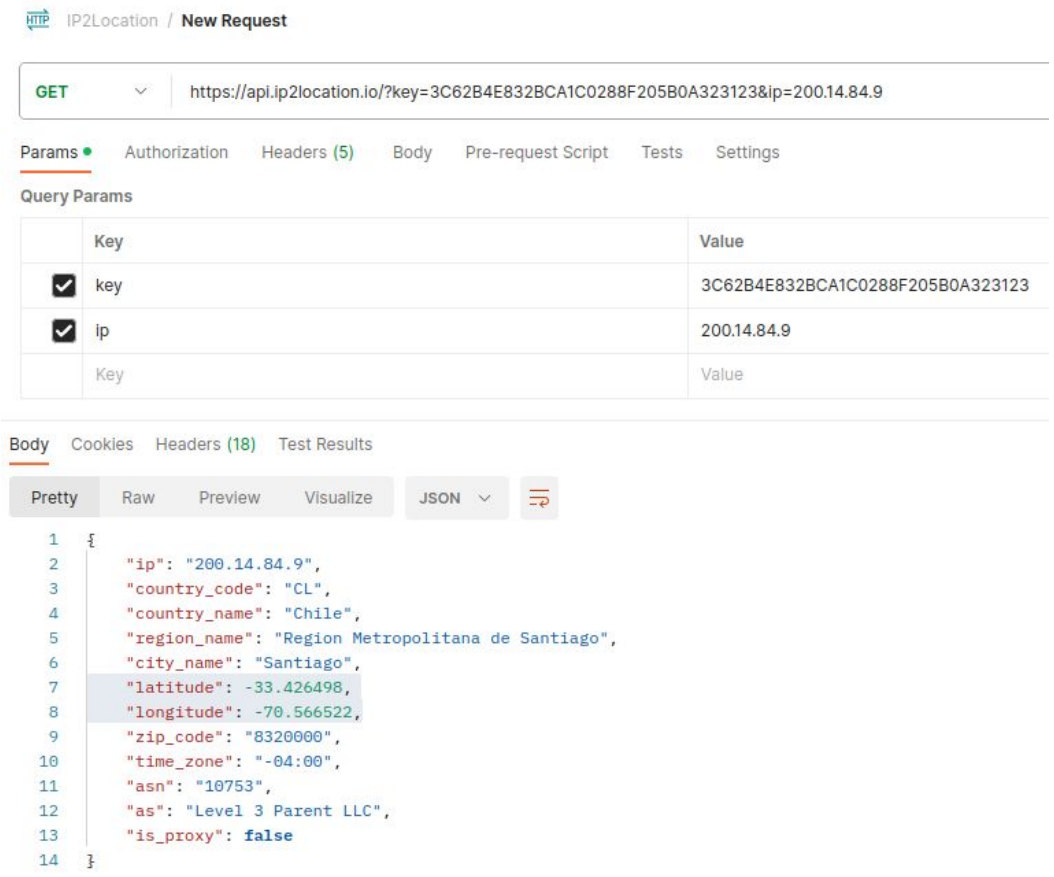
New York				
	MaxMind		IP2Location	
Quantiles	Paid	Free	Paid	Free
0.10	0.73	0.78	2.96	3.04
0.25	1.37	1.47	6.06	6.14
0.50	2.62	2.82	12.04	12.14
0.75	4.95	5.49	30.05	30.48
0.90	9.66	11.02	61.84	63.01

Chicago				
	MaxMind		IP2Location	
Quantiles	Paid	Free	Paid	Free
0.10	0.97	1.02	4.58	4.73
0.25	1.75	1.86	9.79	9.91
0.50	3.31	3.57	23.95	24.28
0.75	6.42	7.10	45.58	45.73
0.90	13.04	16.09	196.43	202.85

Philadelphia				
	MaxMind		IP2Location	
Quantiles	Paid	Free	Paid	Free
0.10	1.13	1.20	4.16	4.19
0.25	2.14	2.27	8.97	9.01
0.50	4.02	4.29	20.87	20.99
0.75	7.57	8.23	39.60	39.71
0.90	13.53	15.03	78.34	78.79

Quantiles of accuracy in kilometers, for each database and city.

IP2Location



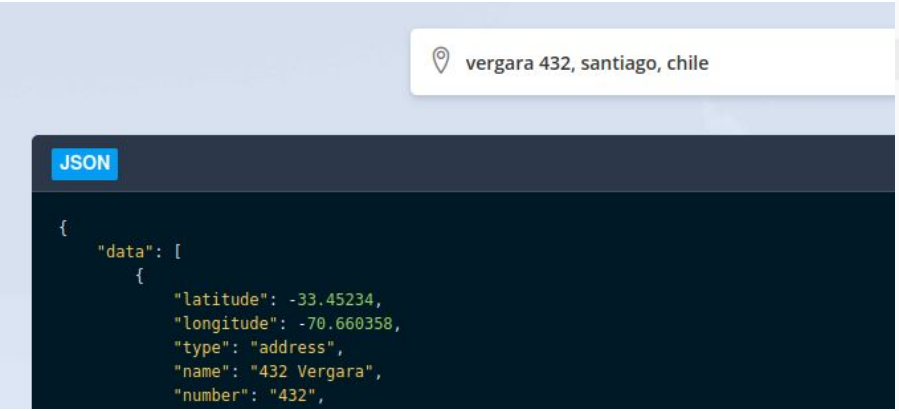
Maxmind

GeoLite2 Endpoints

Service	HTTP Method	Endpoint
Country	GET	https://geolite.info/geoip/v2.1/country/{ip_address}
City	GET	https://geolite.info/geoip/v2.1/city/{ip_address}

```
curl -u "400628:LZN4WT_Emhdn6RBnFdVC8mEHFeHYDXJFh74I_m7k"
"https://geolite.info/geoip/v2.1/city/200.14.84.9?pretty"
```

LatLon 2 Address



https://api.geoapify.com/v1/geocode/reverse?lat=-33.45234&lon=-70.660358&apiKey=

GET https://api.geoapify.com/v1/geocode/reverse?lat=-33.45234&lon=-70.660

Params • Authorization Headers (5) Body Pre-request Script Tests Setting

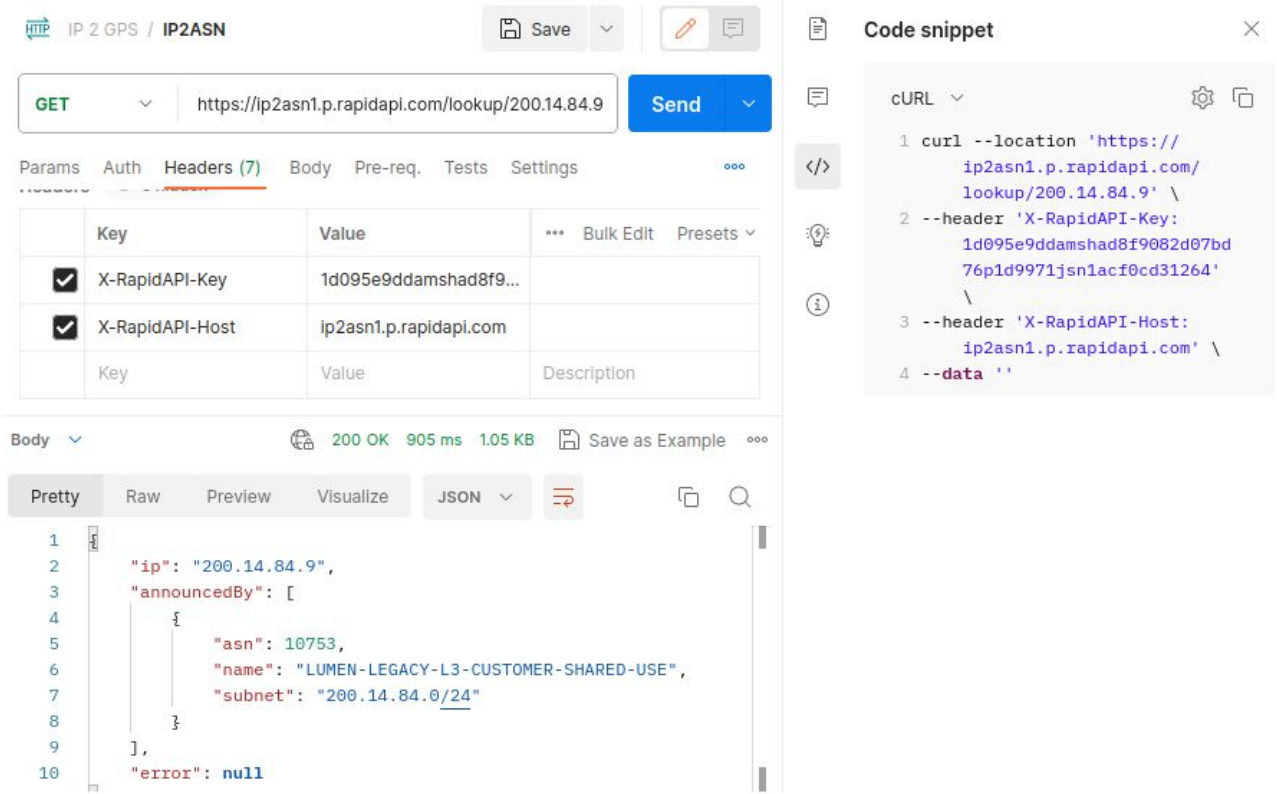
Body Cookies Headers (20) Test Results

Pretty Raw Preview Visualize JSON


```
{
    "type": "FeatureCollection",
    "features": [
        {
            "type": "Feature",
            "properties": {
                "datasource": {
                    "sourcename": "openstreetmap",
                    "attribution": "© OpenStreetMap contributors",
                    "license": "Open Database License",
                    "url": "https://www.openstreetmap.org/copyright"
                },
                "country": "Chile",
                "country_code": "cl",
                "state": "Santiago Metropolitan Region",
                "county": "Provincia de Santiago",
                "city": "Santiago",
                "postcode": "8320000",
                "district": "Barrio Ejército",
                "street": "Ejército Libertador",
                "housenumber": "426",
                "lon": -70.66025305868652,
                "lat": -33.45232215,
```

API Search Engine

ASN

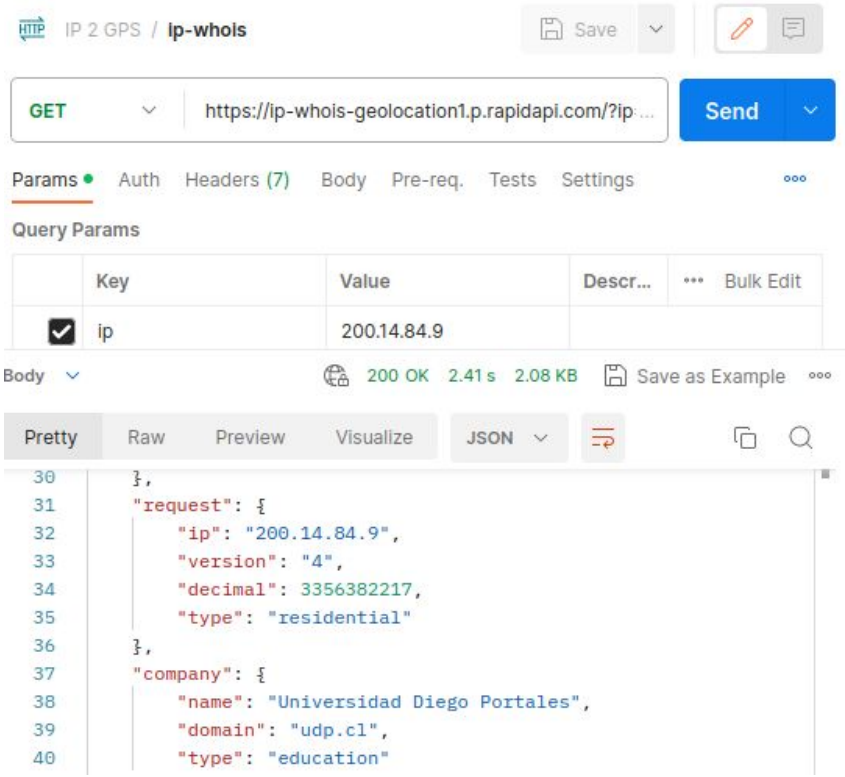

IP 2 GPS / IP2ASN
Save
GET
https://ip2asn1.p.rapidapi.com/lookup/200.14.84.9
Send
Params
Auth
Headers (7)
Body
Pre-req.
Tests
Settings
Key
Value
Bulk Edit
Presets
X-RapidAPI-Key
1d095e9ddamshad8f9...
X-RapidAPI-Host
ip2asn1.p.rapidapi.com
Key
Value
Description
Body
200 OK
905 ms
1.05 KB
Save as Example
Pretty
Raw
Preview
Visualize
JSON
{
"ip": "200.14.84.9",
"announcedBy": [
{
"asn": 10753,
"name": "LUMEN-LEGACY-L3-CUSTOMER-SHARED-USE",
"subnet": "200.14.84.0/24"
}
],
"error": null
Code snippet
cURL
curl --location 'https://ip2asn1.p.rapidapi.com/lookup/200.14.84.9' \
--header 'X-RapidAPI-Key: 1d095e9ddamshad8f9082d07bdp76p1d9971jsn1acf0cd31264' \
--header 'X-RapidAPI-Host: ip2asn1.p.rapidapi.com' \
--data ''

JQuery

```
curl -s --location 'https://ip2asn1.p.rapidapi.com/lookup/
--header 'X-RapidAPI-Key: 1d095e9ddamshad8f9082d07bd76p1d9971jsn1ac
--header 'X-RapidAPI-Host: ip2asn1.p.rapidapi.com' > ip2asn.json; \
> cat ip2asn.json | jq
{
  "ip": "200.14.84.9",
  "announcedBy": [
    {
      "asn": 10753,
      "name": "LUMEN-LEGACY-L3-CUSTOMER-SHARED-USE",
      "subnet": "200.14.84.0/24"
    }
  ],
  "error": null
}
```

```
cat ip2asn.json | jq '.announcedBy[0].asn'
10753
```

IP-whois


IP 2 GPS / ip-whois
Save
GET
https://ip-whois-geolocation1.p.rapidapi.com/?ip
Send
Params
Auth
Headers (7)
Body
Pre-req.
Tests
Settings
Query Params
Key
Value
Descr...
Bulk Edit
ip
200.14.84.9
Body
200 OK
2.41 s
2.08 KB
Save as Example
Pretty
Raw
Preview
Visualize
JSON
},
"request": {
"ip": "200.14.84.9",
"version": "4",
"decimal": 3356382217,
"type": "residential"
},
"company": {
"name": "Universidad Diego Portales",
"domain": "udp.cl",
"type": "education"

Whois information

HURRICANE ELECTRIC INTERNET SERVICES

Search

200.14.84.9

Quick Links

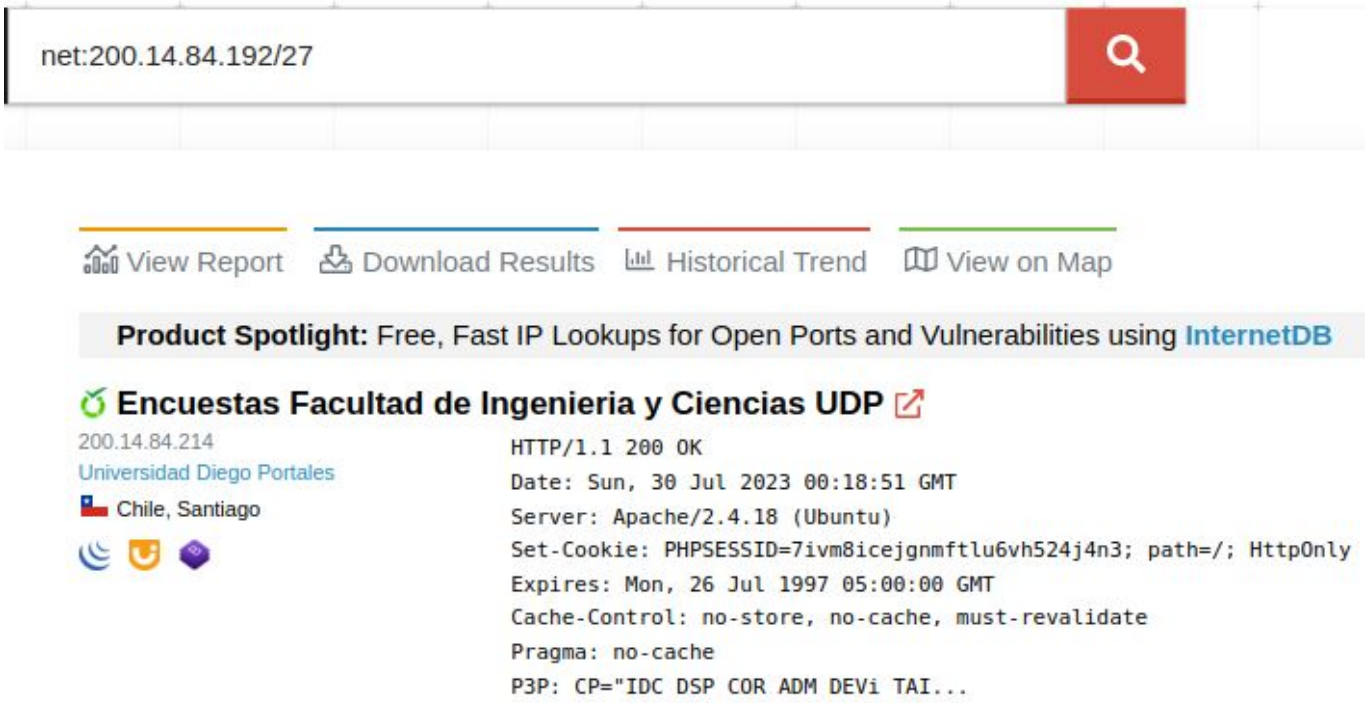
- BGP Toolkit Home
- BGP Prefix Report
- BGP Peer Report
- Exchange Report
- Bogon Routes
- World Report
- Multi Origin Routes
- DNS Report
- Top Host Report
- Internet Statistics
- Looking Glass
- Network Tools App
- Free IPv6 Tunnel
- IPv6 Certification
- IPv6 Progress
- Going Native
- Contact Us

IP Info | Whois | DNS | RBL

```
inetnum:     200.14.84/22
status:      assigned
aut-num:     AS231231
owner:       Universidad Diego Portales
ownerid:     CL-UDPO-LACNIC
responsible: Elas Prez Morales
address:     Manuel Rodriguez sur 333, 415, 3er piso
address:     12345 - Santiago -
country:     CL
phone:       +56 2 6762057 []
owner-c:     GAE13
tech-c:      GAE13
abuse-c:     GAE13
inetrev:     200.14.84/22
nserver:     MBULNES.UDP.CL
nsstat:      20200311 ERR
nslastaa:    20200305
created:     19941117
changed:     20160530

nic-hdl:     GAE13
person:      Gabriel Espinoza
e-mail:      gabriel.espinoza@UDP.CL
address:     Manuel Rodriguez sur 333, 333,
address:     123456789 - santiago - No
country:     CL
phone:       +56 2 6768750 []
created:     20160425
changed:     20160425
```

Shodan search engine



Shodan API

```
curl -s https://api.shodan.io/shodan/host/200.14.84.214\?key=bZyWAS9BqQI6taDPwyhZkzWd9JwIN4am | jq | more
{
  "region_code": "RM",
  "tags": [],
  "ip": 3356382422,
  "area_code": null,
  "domains": [],
  "hostnames": [],
  "country_code": "CL",
  "org": "Universidad Diego Portales",
  "data": [
    {
      "ip": 3356382422,
      "hash": 1212469701,
      "port": 80,
```

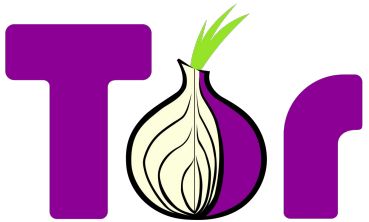
CVE

```
jq -r '.data[0].vulns | keys' 214.json | sort -r | head
  "CVE-2023-25690"
  "CVE-2022-37436",
  "CVE-2022-36760",
  "CVE-2022-31813",
  "CVE-2022-30556",
  "CVE-2022-29404",
  "CVE-2022-28615",
  "CVE-2022-28614",
  "CVE-2022-28330",
  "CVE-2022-26377",
```

TOR + Proxychains4

```
proxychains4 curl -s ifconfig.me
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  ifconfig.me:80  ...  OK
198.251.82.225%
```

```
proxychains4 curl -s https://direccionip.co/ | pup 'span[id="direccion-ip"] text{}'
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  direccionip.co:443  ...  OK
185.181.61.115
```



Open ports

```
sudo proxychains4 masscan -iL ips2.txt -p80,22,443,53 -oJ masscan.json
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2023-08-02 21:27:05 GMT
Initiating SYN Stealth Scan
Scanning 2 hosts [4 ports/host]
cat masscan.json
[
{   "ip": "1.1.1.1",   "timestamp": "1691011625", "ports": [ {"port": 53, "prot
o": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
,
{   "ip": "8.8.8.8",   "timestamp": "1691011625", "ports": [ {"port": 53, "prot
o": "tcp", "status": "open", "reason": "syn-ack", "ttl": 107} ] }
,
{   "ip": "1.1.1.1",   "timestamp": "1691011625", "ports": [ {"port": 80, "prot
o": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
,
{   "ip": "8.8.8.8",   "timestamp": "1691011625", "ports": [ {"port": 443, "pro
to": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
,
{   "ip": "1.1.1.1",   "timestamp": "1691011626", "ports": [ {"port": 443, "pro
to": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
]
```