



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

Latitude

-33.4569

Example: 40.785091

Longitude

-70.6483

Example: -73.968285

Convert

Reverse geocoded address:

Peatonal Coquimbo 1030, 833, Santiago, Metropolitana de Santiago

Santiago Metropolitana de Santiago Chile

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": "technical.isp.",
    "name": "Technical Cont",
    "network": "190.20.0.0/",
    "phone": "+56 26616815"
  },
  "isp": {
    "name": "TELEFÓNICA CHI",
    "domain": "telefonicach",
    "route": "190.20.0.0/16",
    "type": "isp"
  }
}
```

IP2Trace

pip install IP2Trace

● Tokyo, Kanto, Japan

```
%> ip2trace -p 200.14.84.666 -d /usr/share/ip2location/DB4.BIN

IP2Location Geolocation Traceroute (ip2trace) Version 8.0.0
Copyright (c) 2021 IP2Location.com [MIT License]
https://www.ip2location.com/free/traceroute-application

1. 193.27.15.2 2.186 ms ["GB", "United Kingdom of Great Britain and Northern
2. 154.54.89.109 0.835 ms ["JP", "Japan", "Tokyo", "Tokyo", "Cogent Communica
3. 154.54.83.189 128.588 ms ["JP", "Japan", "Tokyo", "Tokyo", "Cogent Communi
4. 154.54.91.126 128.783 ms ["US", "United States of America", "Texas", "El P
5. 200.189.207.14 252.943 ms ["BR", "Brazil", "Sao Paulo", "Cotia", "Cirion T
6. 200.186.40.106 253.176 ms ["BR", "Brazil", "Sao Paulo", "Cotia", "Cirion T
7. 190.217.42.62 253.136 ms ["CL", "Chile", "Region Metropolitana de Santiago
8. 200.189.207.14 274.974 ms ["BR", "Brazil", "Sao Paulo", "Cotia", "Cirion T
9. 200.186.40.102 274.846 ms ["BR", "Brazil", "Sao Paulo", "Cotia", "Cirion T
```

```
↑ ↩ 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



IP2LOCATION

New York				
Quantiles	MaxMind		IP2Location	
	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				
Quantiles	MaxMind		IP2Location	
	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				
Quantiles	MaxMind		IP2Location	
	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

HTTP IP2Location / New Request


GET ▼ <https://api.ip2location.io/?key=3C62B4E832BCA1C0288F205B0A323123&ip=200.14.84.9>

Params ● Authorization Headers (5) Body Pre-request Script Tests Settings

Query Params

	Key	Value
<input checked="" type="checkbox"/>	key	3C62B4E832BCA1C0288F205B0A323123
<input checked="" type="checkbox"/>	ip	200.14.84.9
	Key	Value

Body Cookies Headers (18) Test Results

Pretty Raw Preview Visualize JSON ▼ 

```
1 {
2   "ip": "200.14.84.9",
3   "country_code": "CL",
4   "country_name": "Chile",
5   "region_name": "Region Metropolitana de Santiago",
6   "city_name": "Santiago",
7   "latitude": -33.426498,
8   "longitude": -70.566522,
9   "zip_code": "8320000",
10  "time_zone": "-04:00",
11  "asn": "10753",
12  "as": "Level 3 Parent LLC",
13  "is_proxy": false
14 }
```

Maxmind

🔗 GeoLite2 Endpoints

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

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

LatLon 2 Address

📍 vergara 432, santiago, chile

JSON

```
{
  "data": [
    {
      "latitude": -33.45234,
      "longitude": -70.660358,
      "type": "address",
      "name": "432 Vergara",
      "number": "432",

```

🌐 <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=-70.660358&apiKey=>

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

Body Cookies Headers (20) Test Results

Pretty

Raw

Preview

Visualize

JSON

🔍

```
1
2  "type": "FeatureCollection",
3  "features": [
4    {
5      "type": "Feature",
6      "properties": {
7        "datasource": {
8          "sourcename": "openstreetmap",
9          "attribution": "© OpenStreetMap contributors",
10         "license": "Open Database License",
11         "url": "https://www.openstreetmap.org/copyright"
12       },
13       "country": "Chile",
14       "country_code": "cl",
15       "state": "Santiago Metropolitan Region",
16       "county": "Provincia de Santiago",
17       "city": "Santiago",
18       "postcode": "8320000",
19       "district": "Barrio Ejército",
20       "street": "Ejército Libertador",
21       "housetnumber": "426",
22       "lon": -70.66025305868652,
23       "lat": -33.45232215,
```


API Search Engine



RapidAPI

ASN

HTTP IP 2 GPS / IP2ASN

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
<input checked="" type="checkbox"/> X-RapidAPI-Key	1d095e9ddamshad8f9...			
<input checked="" type="checkbox"/> 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

```
1 {
2   "ip": "200.14.84.9",
3   "announcedBy": [
4     {
5       "asn": 10753,
6       "name": "LUMEN-LEGACY-L3-CUSTOMER-SHARED-USE",
7       "subnet": "200.14.84.0/24"
8     }
9   ],
10  "error": null
```

Code snippet

cURL

```
1 curl --location 'https://
  ip2asn1.p.rapidapi.com/
  lookup/200.14.84.9' \
2 --header 'X-RapidAPI-Key:
  1d095e9ddamshad8f9082d07bd
  76p1d9971jsn1acf0cd31264' \
3 --header 'X-RapidAPI-Host:
  ip2asn1.p.rapidapi.com' \
4 --data ''
```

JQuery

```
⌘ ~ curl -s --location 'https://ip2asn1.p.rapidapi.com/lookup/;  
--header 'X-RapidAPI-Key: 1d095e9ddamshad8f9082d07bd76p1d9971jsn1ac1  
--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

HTTP IP 2 GPS / ip-whois Save Edit Comments

GET Send

Params Auth Headers (7) Body Pre-req. Tests Settings ...

Query Params

	Key	Value	Descr...	...	Bulk Edit
<input checked="" type="checkbox"/>	ip	200.14.84.9			

Body ... 200 OK 2.41 s 2.08 KB Save as Example ...

Pretty Raw Preview Visualize JSON ... Copy Search

```
30  },
31  "request": {
32    "ip": "200.14.84.9",
33    "version": "4",
34    "decimal": 3356382217,
35    "type": "residential"
36  },
37  "company": {
38    "name": "Universidad Diego Portales",
39    "domain": "udp.cl",
40    "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: Elías Prez Morales
address: Manuel Rodríguez 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 Rodríguez sur 333, 333,
address: 123456789 - Santiago - No
country: CL
phone: +56 2 6768750 []
created: 20160425
changed: 20160425



Shodan search engine

net:200.14.84.192/27

Q

[View Report](#)[Download Results](#)[Historical Trend](#)[View on Map](#)

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

Encuestas Facultad de Ingenieria y Ciencias UDP

200.14.84.214

[Universidad Diego Portales](#)



Chile, Santiago



HTTP/1.1 200 OK

Date: Sun, 30 Jul 2023 00:18:51 GMT

Server: Apache/2.4.18 (Ubuntu)

Set-Cookie: PHPSESSID=7ivm8icejgnmftlu6vh524j4n3; path=/; HttpOnly

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Cache-Control: no-store, no-cache, must-revalidate

Pragma: no-cache

P3P: CP="IDC DSP COR ADM DEVi TAI...

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",
```

CVExploits Search

Your comprehensive database for CVE exploits from across the internet.

Search : CVE-2020-2125, or product/software ex: apache

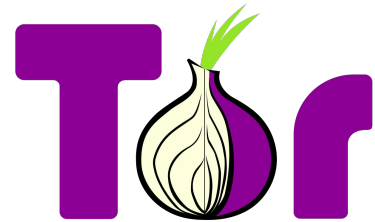


Found 1 Results for: 2023-25690

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

```
root@kali:~# 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]
root@kali:~# cat masscan.json
[
  {
    "ip": "1.1.1.1",
    "timestamp": "1691011625",
    "ports": [ {"port": 53, "proto": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
  ,
  {
    "ip": "8.8.8.8",
    "timestamp": "1691011625",
    "ports": [ {"port": 53, "proto": "tcp", "status": "open", "reason": "syn-ack", "ttl": 107} ] }
  ,
  {
    "ip": "1.1.1.1",
    "timestamp": "1691011625",
    "ports": [ {"port": 80, "proto": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
  ,
  {
    "ip": "8.8.8.8",
    "timestamp": "1691011625",
    "ports": [ {"port": 443, "proto": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
  ,
  {
    "ip": "1.1.1.1",
    "timestamp": "1691011626",
    "ports": [ {"port": 443, "proto": "tcp", "status": "open", "reason": "syn-ack", "ttl": 55} ] }
]
```

