IP Address Research: 5 Ways to Do It Explained

Posted on June 9, 2021



Personalization is the way to go when it comes to targeted marketing and advertising. Customers, existing and potential alike, want to feel that the brands they support care about their needs and try to predict what they might want. That's what makes IP address research critical for digital marketers and advertisers.

But they aren't the only ones who can benefit from IP geolocation data, cybersecurity pros, fraud protection agents, and market researchers do, too. Every computer or mobile device, after all, has a designated IP address that helps today's companies and individuals pinpoint where their strongest markets are, identify where threats likely come from, detect potentially fraudulent transactions, and predict consumption patterns and trends.

5 Lookups Explained for IP Address Research

There are tons of ways to locate an Internet user and we'll discuss them in greater detail in the next sections. You can choose one or more of them to improve your IP address research for any of your business- or cybersecurity-related processes.

Option #1: Using a Bulk IP Lookup Tool

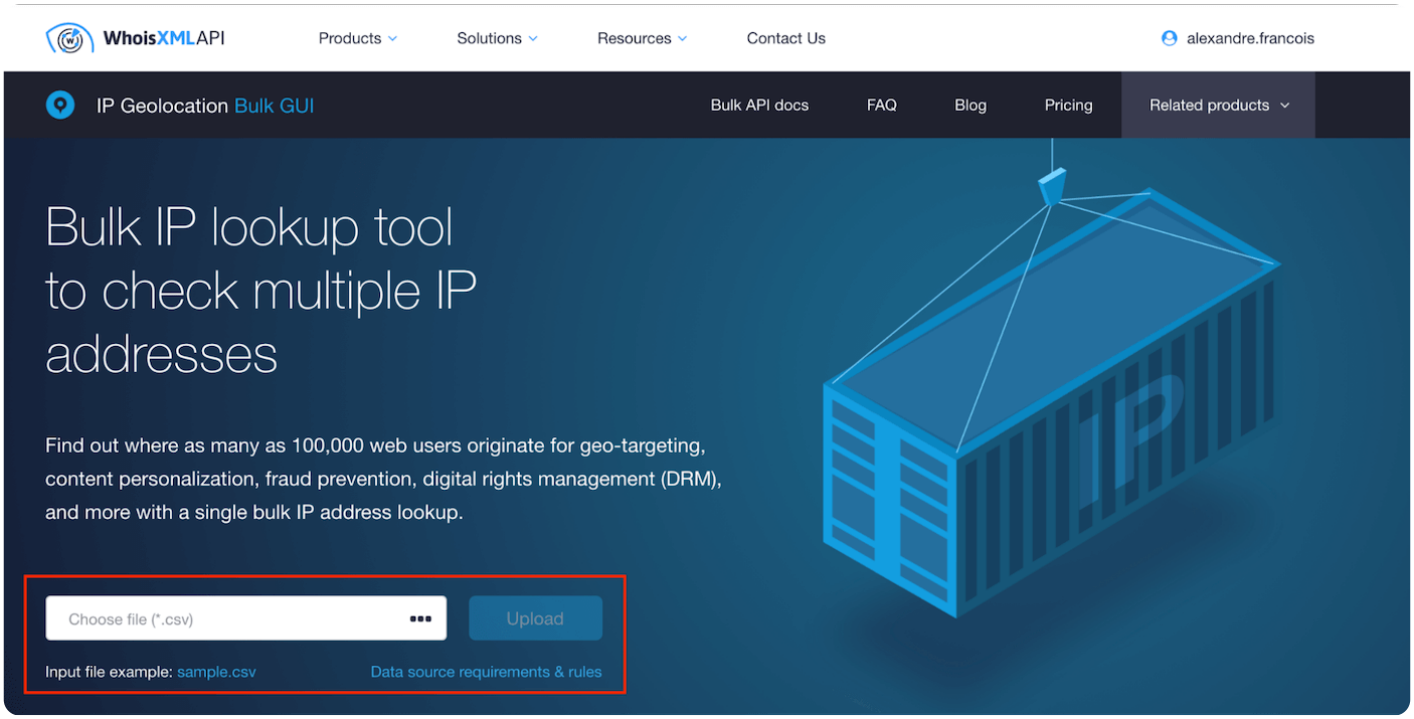
It's often the norm for any company that sells products online to keep a customer database. That's how marketers keep track of purchases, determine their loyal shoppers, personalize content, and take advantage of strategies like geo-targeting.

Logging IP addresses that come into contact with one's network, meanwhile, is also a given now since cyberattacks are widespread. IP address research is one of the means cybersecurity analysts use to determine an attacker's possible location, identify cybercrime hotspots, prevent fraud, and block access to and from threat sources.

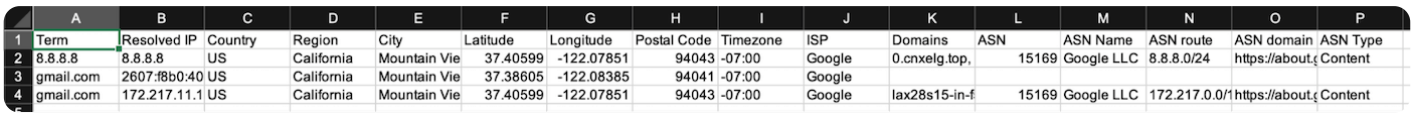
A bulk IP lookup tool is an easy way to do IP address research. You can perform one in two ways.

You can upload a comma-separated values (CSV) file containing all of the IP addresses you wish to query into the input field and click **Upload**. Alternatively, you can copy and paste all of the IP addresses from a network log, for instance, into the input field and click **Upload**. Wait a few

minutes and download the results in CSV format.



You will get an IP address list like the one below, which tells you the IP addresses' corresponding countries; regions or states; cities; latitude and longitude coordinates; postal codes; time zones; Internet service providers (ISPs); domain resolutions (maximum of three); and Autonomous System (AS) numbers, routes, domains, and types.

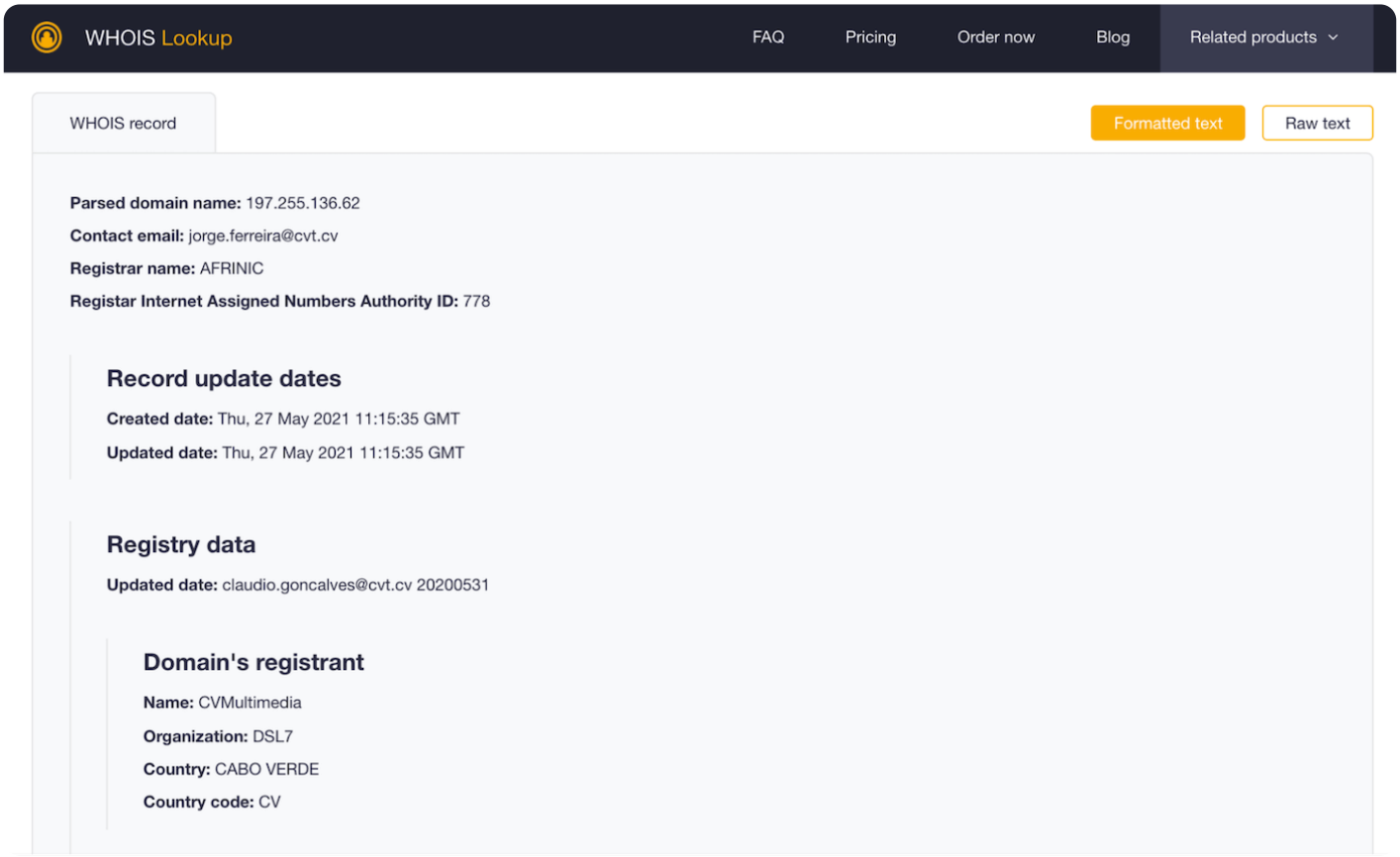


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Term	Resolved IP	Country	Region	City	Latitude	Longitude	Postal Code	Timezone	ISP	Domains	ASN	ASN Name	ASN route	ASN domain	ASN Type
2	8.8.8.8	8.8.8.8	US	California	Mountain Vie	37.40599	-122.07851	94043	-07:00	Google	0.cnxelg.top,	15169	Google LLC	8.8.8.0/24	https://about.(	Content
3	gmail.com	2607:f8b0:40	US	California	Mountain Vie	37.38605	-122.08385	94041	-07:00	Google						
4	gmail.com	172.217.11.1	US	California	Mountain Vie	37.40599	-122.07851	94043	-07:00	Google	lax28s15-in-f	15169	Google LLC	172.217.0.0/1	https://about.(	Content

Option #2: Using a WHOIS Lookup Tool

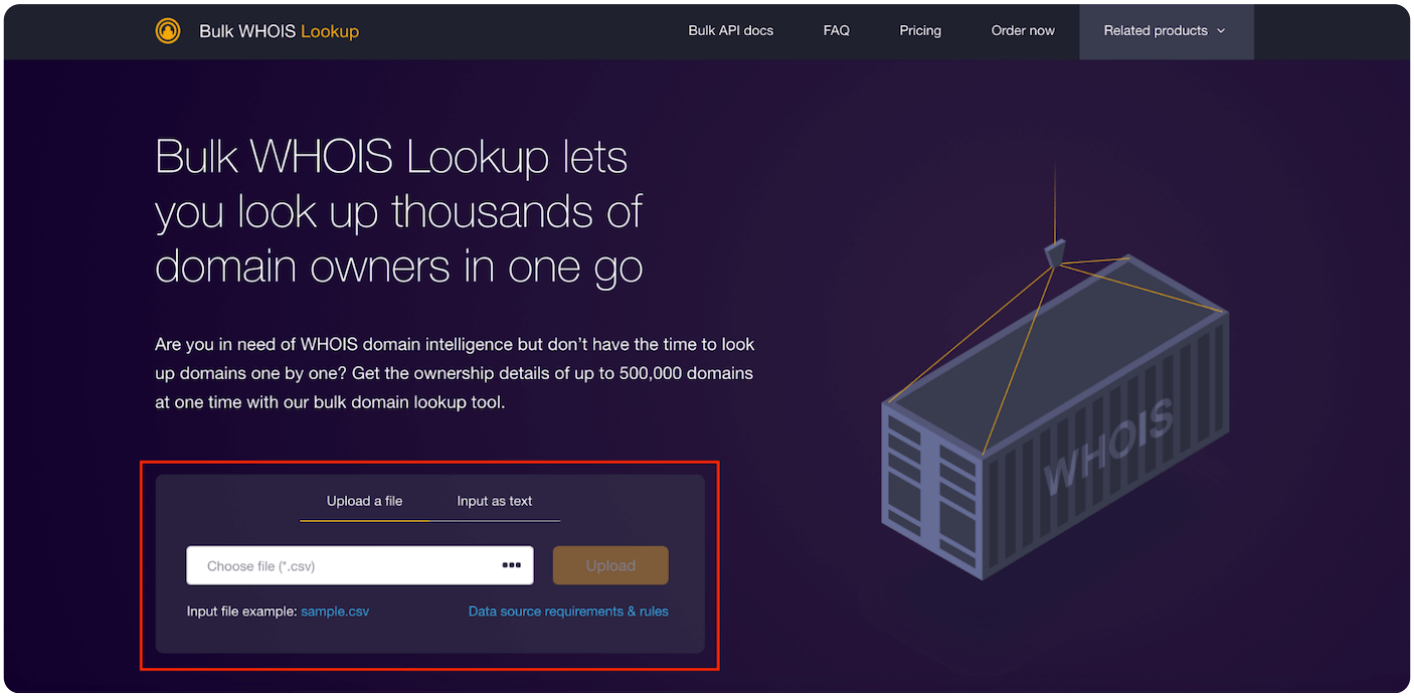
While WHOIS searches are more typically used to obtain domain ownership information, it is also

useful for IP address research. An IP address search on a WHOIS lookup tool will tell you who or what company administrates it. Registry data can be useful in cybersecurity when it comes to reporting abuse.



Option #3: Using a Bulk IP WHOIS Lookup Tool

Bulk WHOIS lookups provide the same results as an ordinary WHOIS search with one major difference—you can query as many as 500,000 IP addresses at one time. You can use it the same way you would a bulk IP lookup tool. Upload a CSV file containing the IP addresses you'd like to query using the input field. Copying and pasting IP addresses into the field works as well.



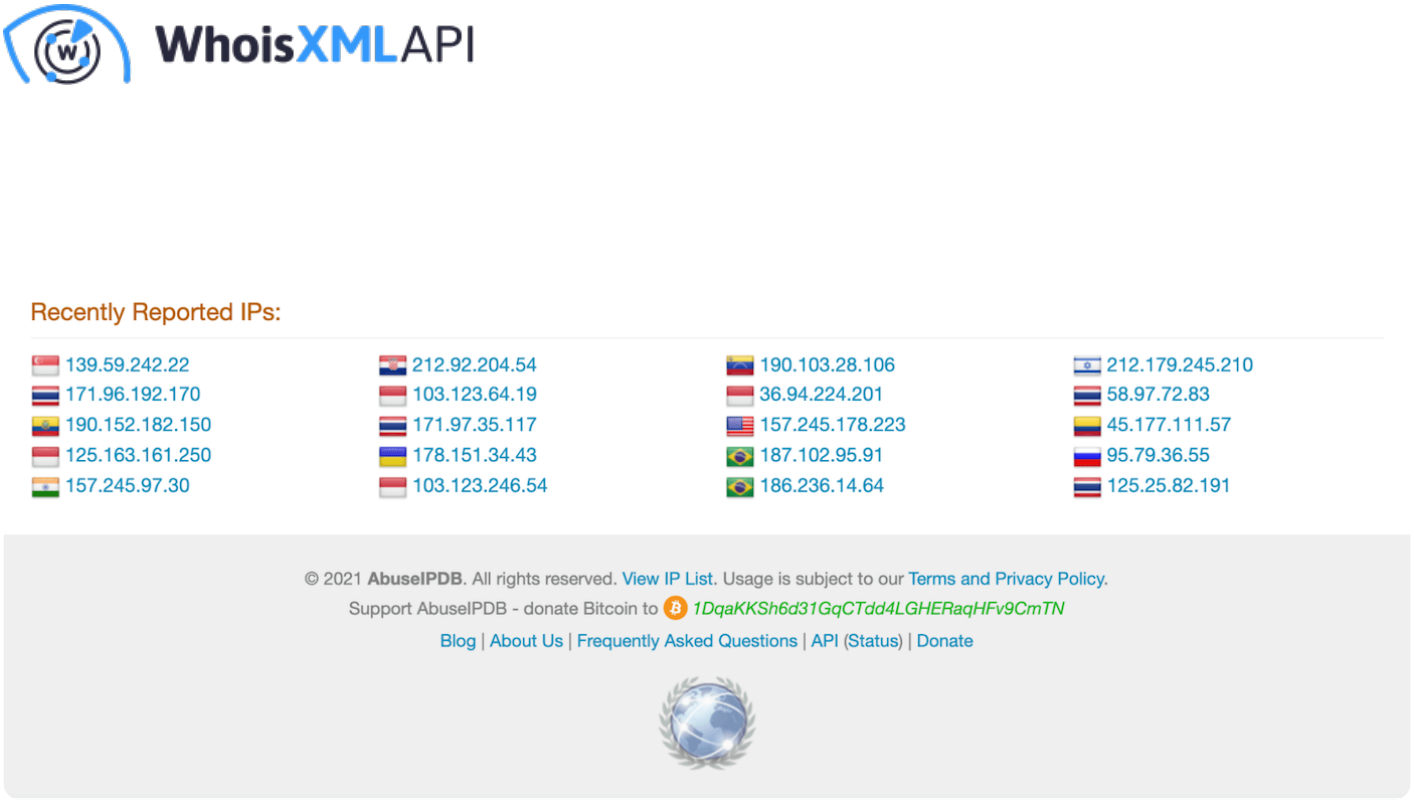
Wait for the processing to finish and download the results. It should look something like this:

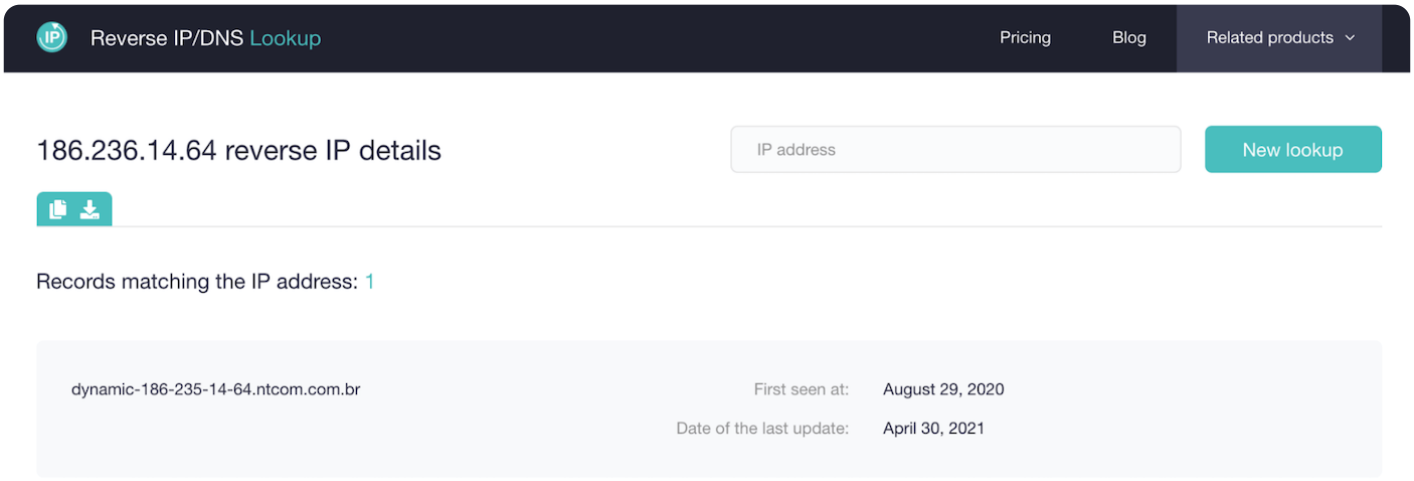
domainName	registrarName	contactEmail	whoisServer	domainAvailability	nameServers	createdDate	updatedDate	expiresDate	standardRegCreatedDate
171.96.192.170	APNIC	abuse@trueinternet.co.th					2011-12-06T00:10:15Z		
125.163.161.250	APNIC	abuse@telkom.co.id					2015-05-27T03:33:18Z		
171.97.35.117	APNIC	abuse@trueinternet.co.th					2011-12-06T00:10:15Z		
186.236.14.64	LACNIC	cert@cert.br				20100914	20100914		
157.245.97.30	ARIN	abuse@digitalocean.com				2019-05-09	2020-04-03		2019-05-09 00:00:00 UTC
157.245.178.223	ARIN	abuse@digitalocean.com				2019-05-09	2020-04-03		2019-05-09 00:00:00 UTC
187.102.95.91	LACNIC	denilson@bnet.com.br				20091113	20130307		
125.25.82.191	APNIC	abuse@totisp.net					2010-07-25T08:36:03Z		
139.59.242.22	APNIC	abuse@digitalocean.com					2015-04-02T20:27:52Z		
103.123.246.54	APNIC	abuse@moratelindo.co.id					2018-11-23T09:28:35Z		
178.151.34.43	RIPE	abuse@triolan.com.ua				2016-10-19T13:01:10Z	2019-07-22T15:15:24Z		2016-10-19 00:00:00 UTC
45.177.111.57	LACNIC	amortigo@ims.net.co				20160905	20191121		
212.179.245.210	RIPE	abuse@bezeqint.net				1970-01-01T00:00:00Z	2004-10-31T13:07:24Z		1970-01-01 00:00:00 UTC
190.152.182.150	LACNIC	anabel.carrera@cnt.gob.ec				20030402	20190325		
190.103.28.106	LACNIC	lacnic@fibextelecom.net				20111228	20210519		
95.79.36.55	ORG-CNN1-RIPE	ripe@ertelecom.ru				2007-12-19T08:19:13Z	2019-10-16T12:10:39Z		2007-12-19 00:00:00 UTC
212.92.204.54	ORG-VGd1-RIPE	l2@A1.hr				2008-08-28T09:54:24Z	2008-08-28T09:54:24Z		2008-08-28 00:00:00 UTC
58.97.72.83	APNIC	abuse@trueinternet.co.th					2011-12-06T00:10:15Z		
36.94.224.201	ORG-TI10-AP	abuse@telkom.co.id					2013-12-10T08:18:41Z		

Option #4: Using a Reverse IP/DNS Lookup Tool

Passive Domain Name System (DNS) data such as that from reverse IP/DNS lookup tools can help with IP address research as well. The information you gain from such searches can be useful in additional threat artifact discovery, asset mapping, and indicators of compromise (IoCs) list expansion.

Given an IP address, you can identify all of the domains that resolved to it at one point in time. If you take the malicious IP address 186[.]236[.]14[.]64 identified by AbuseIPDB as of 27 May 2021, for instance, you would know that it's connected to the subdomain dynamic-186-235-14-64[.]ntcom[.]com[.]br.





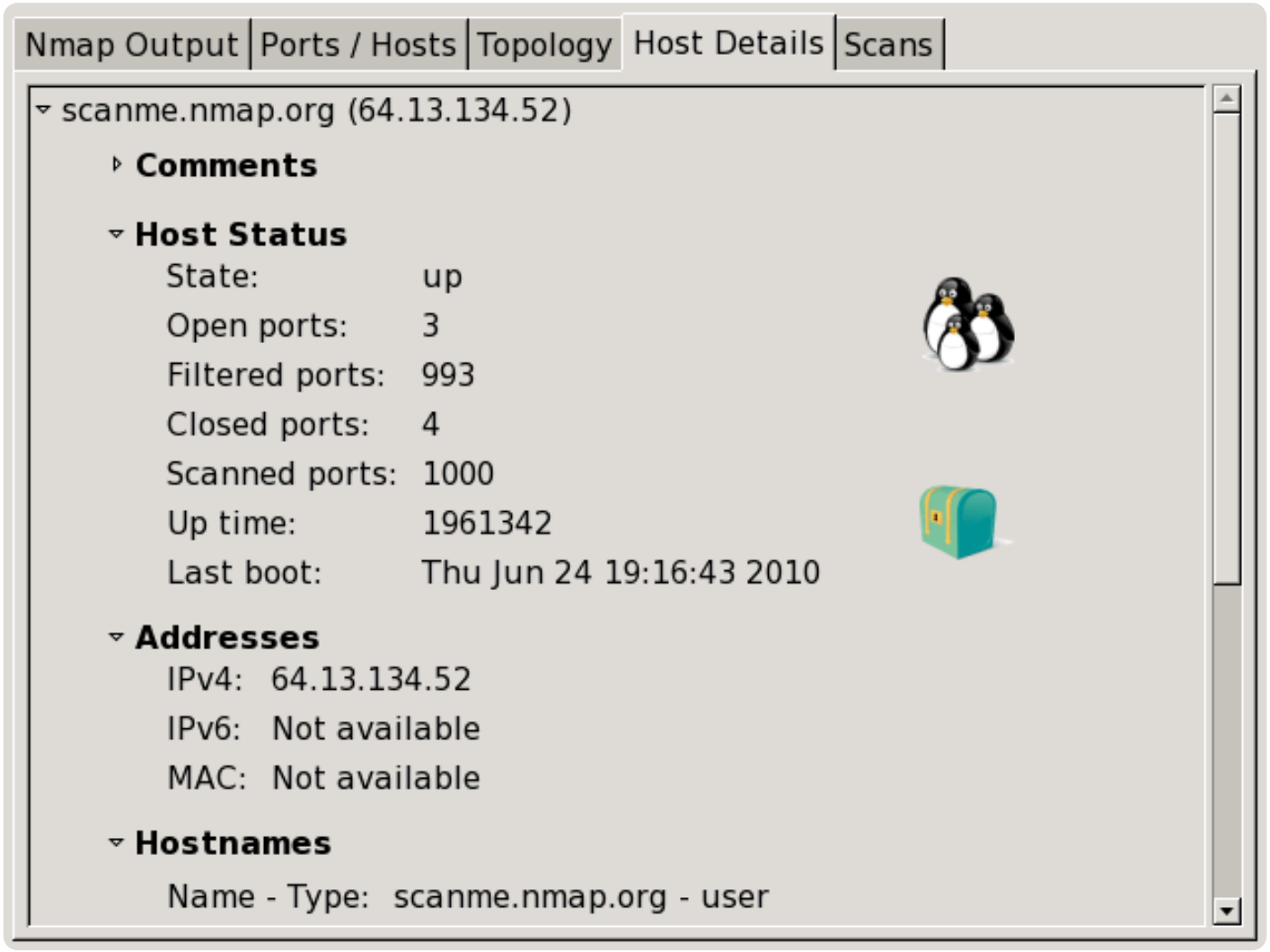
If you would like to avoid the threats related to 186[.]236[.]14[.]64, therefore, avoiding dealings with dynamic-186-235-14-64[.]ntcom[.]com[.]br should become part of your cybersecurity strategy.

Option #5: Using Nmap

Nmap is essentially an open-source network mapper and port scanner but is also useful for IP address research. To perform an IP address search, follow these steps:

- Download the version that's compatible with your system Nmap's website.
- Open the program. Type # **nmap -sL <IP address>**.

You should see a result that looks like this:



Making Your Choice

Among the ways to conduct IP address research mentioned above, it is generally more advantageous to use bulk options if you need to query thousands of IP addresses at one time. Bulk IP Lookup, for example, can give you the geolocation data of up to 100,000 users in one go while Bulk IP WHOIS Lookup can do so for 500,000 IP addresses at once.

The results from both Bulk IP Lookup and Bulk IP WHOIS Lookup also come in a format that you can easily correlate with other databases. You can also create charts using the IP address

research data you collated by simply saving the CSV file as a spreadsheet using programs like Excel (on Windows) or Numbers (on macOS).

Your choice of IP address solution depends on your business requirements. If you wish to simply find the physical locations of thousands of users, use a bulk IP lookup tool. If you need to identify who is in charge of a particular IP address, you can opt for IP WHOIS Lookup or Bulk IP WHOIS Lookup. What's more, if you're mapping a potential cyber attacker's infrastructure, you may choose Nmap or passive Domain Name System (DNS) lookup tools like Reverse IP Lookup.