



# *Simple English* WIKIPEDIA

## INFORMATION GATHER ABOUT WIKIPEDIA.ORG

INFO FROM COMMANDS, INFO FROM DIFF WEBSITES

██████████ | CERTIFIED ETHICAL HACKER | July 28, 2024

## INFORMATION GATHER FROM COMMANDS:

### 1)WHOIS COMMANDS:

Domain Name: wikipedia.org

Registry Domain ID: d1a549fd3c4dd389c3c575a889efb1-LROR

Registrar WHOIS Server: <http://whois.markmonitor.com>

Registrar URL: <http://www.markmonitor.com>

Updated Date: 2023-12-17T09:18:25Z

Creation Date: 2001-01-13T00:12:14Z

Registry Expiry Date: 2025-01-13T00:12:14Z

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email: [Abusecomplaints@markmonitor.com](mailto:Abusecomplaints@markmonitor.com)

Registrar Abuse Contact Phone: +1.2083895740

Domain Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>

Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>

Domain Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>

Registrant Organization: Wikimedia Foundation, Inc.

Registrant State/Province: CA

Registrant Country: US

Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Name Server: ns0.wikimedia.org

Name Server: ns1.wikimedia.org

Name Server: ns2.wikimedia.org

## 2)HOST COMMAND:

Wikipedia.org has address **103.102.166.224**

wikipedia.org has IPv6 address **2001:DF2:E500:ED1A::1**

wikipedia.org mail is handled by 10 mx-in1001.wikimedia.org.

wikipedia.org mail is handled by 10 mx-in2001.wikimedia.org.

## 3)NSLOOKUP -TYPE=TXT COMMANDS:

Server:192.168.44.2

Address: 192.168.44.2#53

## 4)DNSENUM COMMANDS:

----- wikipedia.org -----

### - Host's addresses:

Wikipedia.org.	5	IN	A	103.102.166.224
----------------	---	----	---	-----------------

### - Name Servers:

nso.wikimedia.org.	5	IN	A	208.80.154.238
--------------------	---	----	---	----------------

ns1.wikimedia.org.	5	IN	A	208.80.153.231
--------------------	---	----	---	----------------

ns2.wikimedia.org.	5	IN	A	198.35.27.27
--------------------	---	----	---	--------------

### - Mail (MX) Servers:

mx-in1001.wikimedia.org.	5	IN	A	208.80.155.102
--------------------------	---	----	---	----------------

mx-in2001.wikimedia.org.	5	IN	A	208.80.153.75
--------------------------	---	----	---	---------------

### - Trying Zone Transfers and getting Bind Versions:

Trying Zone Transfer for wikipedia.org on nso.wikimedia.org ...

AXFR record query failed: NOTIMP

### - Brute forcing with /usr/share/dnsenum/dns.txt:

av.wikipedia.org.	5	IN	CNAME	dyna.wikimedia.org.
-------------------	---	----	-------	---------------------

be.wikipedia.org.	5	IN	CNAME	dyna.wikimedia.org.
-------------------	---	----	-------	---------------------

dyna.wikimedia.org.	5	IN	A	103.102.166.224
---------------------	---	----	---	-----------------

### - wikipedia.org class C

netranges: 103.102.166.0/24

- Performing reverse lookup on 256 ip addresses:

- o results out of 256 IP addresses.

- wikipedia.org ip blocks:

- done.

## 5)AMASS ENUM -D COMMAND:

(ONLY IP ADDRESS ARE SHOWN HERE)

wikipedia.org (FQDN) --> a\_record --> 185.15.59.224 (IPAddress)

wikipedia.org (FQDN) --> aaaa\_record --> 2001:df2:e500:edia::1 (IPAddress)

mx-in1001.wikimedia.org (FQDN) --> a\_record --> 208.80.155.102 (IPAddress)

mx-in1001.wikimedia.org (FQDN) --> aaaa\_record --> 2620:0:861:4:208:80:155:102 (IPAddress)

185.15.59.0/24 (Netblock) --> contains --> 185.15.59.224 (IPAddress)

ns1.wikimedia.org (FQDN) --> a\_record --> 208.80.153.231 (IPAddress)

dyna.wikimedia.org (FQDN) --> a\_record --> 103.102.166.224 (IPAddress)

dyna.wikimedia.org (FQDN) --> aaaa\_record --> 2001:df2:e500:edia::1 (IPAddress)

dyna.wikimedia.org (FQDN) --> a\_record --> 208.80.154.224 (IPAddress)

dyna.wikimedia.org (FQDN) --> aaaa\_record --> 2a02:ec80:300:edia::1 (IPAddress)

208.80.152.0/22 (Netblock) --> contains --> 208.80.155.102 (IPAddress)

208.80.152.0/22 (Netblock) --> contains --> 208.80.153.231 (IPAddress)

208.80.152.0/22 (Netblock) --> contains --> 208.80.154.224 (IPAddress)

2620:0:860::/46 (Netblock) --> contains --> 2620:0:861:4:208:80:155:102 (IPAddress)

103.102.166.0/24 (Netblock) --> contains --> 103.102.166.224 (IPAddress)

2a02:ec80::/32 (Netblock) --> contains --> 2a02:ec80:300:edia::1 (IPAddress)

nso.wikimedia.org (FQDN) --> a\_record --> 208.80.154.238 (IPAddress)

ns2.wikimedia.org (FQDN) --> a\_record --> 198.35.27.27 (IPAddress)

mx-in2001.wikimedia.org (FQDN) --> a\_record --> 208.80.153.75 (IPAddress)

mx-in2001.wikimedia.org (FQDN) --> aaaa\_record --> 2620:0:860:3:208:80:153:75 (IPAddress)

208.80.152.0/22 (Netblock) --> contains --> 208.80.153.75 (IPAddress)

208.80.152.0/22 (Netblock) --> contains --> 208.80.154.238 (IPAddress)

2620:0:860::/46 (Netblock) --> contains --> 2620:0:860:3:208:80:153:75 (IPAddress)

198.35.26.0/23 (Netblock) --> contains --> 198.35.27.27 (IPAddress)

## 6)NMAP COMMAND:

Starting Nmap 7.94SVN ( <https://nmap.org> ) at 2024-07-27 00:25 EDT

Nmap scan report for wikipedia.org (103.102.166.224)

Host is up (0.15s latency).

Other addresses for wikipedia.org (not scanned): 2001:df2:e500:edia::1

rDNS record for 103.102.166.224: text-lb.eqsin.wikimedia.org

Not shown: 998 filtered tcp ports (no-response)

– PORT STATE SERVICE

80/ tcp open http  
443/ tcp open https

## INFORMATION GATHER FROM WEBSITES:

### 1) IPINFO.IO WEBSITE:

- ip: "103.102.166.224", hostname: "text-lb.eqsin.wikimedia.org",  
city: "Singapore", region: "Singapore",  
country: "SG", loc: "1.2897,103.8501",  
org: "AS14907 Wikimedia Foundation Inc.", postal: "018989",  
timezone: "Asia/Singapore",  
- asn: Object,  
ASN: "AS14907", name: "Wikimedia Foundation Inc.",  
domain: "wikimediafoundation.org", route: "103.102.166.0/24",  
type: "hosting",  
- company: Object,  
name: "Wikimedia Foundation, Inc.", domain: "wikimedia.org",  
- privacy: Object,  
vpn: false, proxy: false, tor: false, relay: false, hosting: true,  
- abuse: Object,  
address: "1 Montgomery Street, Suite 1600, San Francisco, CA 94104, US",  
country: "US", email: "abuse@wikimedia.org",  
name: "ABUSE WIKIMEDIAAP", network: "103.102.166.0/24",  
phone: "+0000000000",

### 2) BGP.HE.NET WEBSITE:

#### WHOIS INFORMATION FROM WEBSITE:

ASNumber: 14907AS      Name: WIKIMEDIA      ASHandle: AS14907  
RegDate: 2006-09-27      Updated: 2012-03-02  
Ref: <https://rdap.arin.net/registry/autnum/14907>  
OrgName: Wikimedia Foundation Inc.      OrgId: WIKIM

Address: 1 Montgomery Street Address: Suite 1600 PostalCode: 94104

Ref : <https://rdap.arin.net/registry/entity/WIKIM> OrgAbuseHandle: WNA11-ARIN

OrgAbuseName: Wikimedia Network Abuse OrgAbusePhone: +1-415-839-6885

OrgAbuseEmail: [abuse@wikimedia.org](mailto:abuse@wikimedia.org)

OrgAbuseRef: <https://rdap.arin.net/registry/entity/WNA11-ARIN>

OrgTechHandle: YOUNS-ARIN OrgTechName: Younsi, Arzhel

OrgTechPhone: +1-415-839-6885 OrgTechEmail: ayounsi@wikimedia.org

OrgTechRef: <https://rdap.arin.net/registry/entity/YOUNS-ARIN>

OrgNOCHandle: WIKIM-ARIN OrgNOCName: Wikimedia NOC

OrgNOCPhone: +1-415-839-6885 OrgNOCEmail: noc@wikimedia.org

OrgNOCRef: <https://rdap.arin.net/registry/entity/WIKIM-ARIN>

OrgTechHandle: MBE96-ARIN OrgTechName: Bergsma, Mark

OrgTechPhone: +1-415-839-6885 OrgTechEmail: mark@wikimedia.org

OrgTechRef: <https://rdap.arin.net/registry/entity/MBE96-ARIN>







OrgTechHandle: MOONE85-ARIN OrgTechName: Mooney, Cathal

OrgTechPhone: +1-415-839-6885 OrgTechEmail: cmooney@wikimedia.org

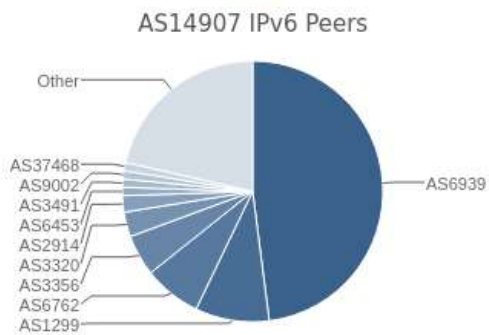
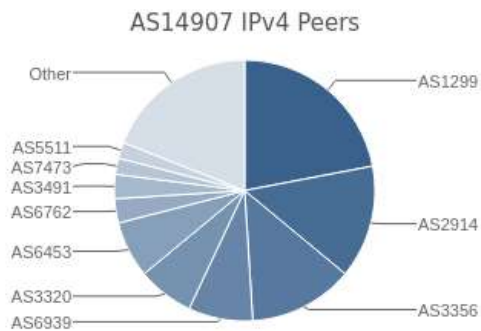
OrgTechRef: <https://rdap.arin.net/registry/entity/MOONE85-ARIN>

Prefix		Description	Visibility
<a href="#">103.102.166.0/24</a>		Wikimedia Foundation, Inc.	 100% 648/648
<a href="#">185.15.56.0/24</a>		Wikimedia cloud eqiad	 100% 648/648
<a href="#">185.15.57.0/24</a>		Wikimedia Foundation, Inc.	 100% 648/648
<a href="#">185.15.58.0/24</a>		Wikimedia Foundation, Inc.	 100% 648/648
<a href="#">185.15.59.0/24</a>		Wikimedia esams infra	 100% 647/648
<a href="#">185.71.138.0/24</a>		Wikimedia Foundation, Inc.	 100% 648/648
<a href="#">195.200.68.0/24</a>		Wikimedia Foundation, Inc.	 100% 648/648
<a href="#">198.35.26.0/24</a>		Wikimedia Foundation Inc.	 100% 648/648
<a href="#">198.35.27.0/24</a>		Wikimedia Foundation Inc.	 100% 648/648
<a href="#">208.80.152.0/23</a>		Wikimedia Foundation Inc.	 100% 648/648
<a href="#">208.80.154.0/23</a>		Wikimedia Foundation Inc.	 100% 648/648

## INTERNET EXCHANGE(IE) INFO:

Exchange		CC	City	IPv4	IPv6
<a href="#">AMS-IX</a>		NL	Amsterdam	80.249.209.176	2001:7fb:1::a501:4907:1
<a href="#">BBIX Singapore</a>		SG	Singapore	103.231.152.197	2001:df5:b800:bb00:0:1:4907:1
<a href="#">DE-CIX Dallas</a>		US	Dallas	206.53.202.101	2001:504:61::3a3b:0:1
<a href="#">DE-CIX Marseille</a>		FR	Marseille	185.1.47.125	2001:7fb:36::3a3b:0:1
<a href="#">Equinix Ashburn</a>		US	Ashburn	206.126.236.106 206.126.236.221	2001:504:0:2:0:1:4907:1 2001:504:0:2:0:1:4907:2
<a href="#">Equinix Chicago</a>		US	Chicago	208.115.136.238	2001:504:0:4:0:1:4907:1
<a href="#">Equinix Dallas</a>		US	Dallas	206.223.118.197	2001:504:0:5:0:1:4907:1
<a href="#">Equinix Palo Alto</a>		US	Palo Alto	198.32.176.214	2001:504:d:1:4907:1
<a href="#">Equinix San Jose</a>		US	San Jose		2001:504:0:1:0:1:4907:1
<a href="#">Equinix Singapore</a>		SG	Singapore	27.111.228.186	2001:ee8:4::1:4907:1
<a href="#">France-IX Marseille</a>		FR	Marseille	37.49.232.11	2001:7fb:34:5::11
<a href="#">NL-IX</a>		NL	Amsterdam	193.239.119.50	2001:7fb:13::a501:4907:1
<a href="#">PTT São Paulo</a>		BR	São Paulo	187.16.212.158	2001:12fb::212:158
<a href="#">SFMIX</a>		US	San Francisco	206.197.187.82	2001:504:30::ba01:4907:1
<a href="#">SGIX</a>		SG	Singapore	103.16.102.187	2001:ee8:12:100::187

## AS INFORMATION






ASN	Name
<a href="#">AS1299</a>	<a href="#">Arelion Sweden AB</a>
<a href="#">AS2914</a>	<a href="#">NTT America, Inc.</a>
<a href="#">AS3356</a>	<a href="#">Level 3 Parent, LLC</a>
<a href="#">AS6939</a>	<a href="#">Hurricane Electric LLC</a>
<a href="#">AS3320</a>	<a href="#">Deutsche Telekom AG</a>
<a href="#">AS6453</a>	<a href="#">TATA COMMUNICATIONS (AMERICA) INC</a>
<a href="#">AS6762</a>	<a href="#">TELECOM ITALIA SPARKLE S.p.A.</a>
<a href="#">AS3491</a>	<a href="#">PCCW Global</a>
<a href="#">AS7473</a>	<a href="#">Singapore Telecommunications Ltd</a>
<a href="#">AS5511</a>	<a href="#">Orange S.A.</a>

ASN	Name
<a href="#">AS6939</a>	<a href="#">Hurricane Electric LLC</a>
<a href="#">AS1299</a>	<a href="#">Arelion Sweden AB</a>
<a href="#">AS6762</a>	<a href="#">TELECOM ITALIA SPARKLE S.p.A.</a>
<a href="#">AS3356</a>	<a href="#">Level 3 Parent, LLC</a>
<a href="#">AS3320</a>	<a href="#">Deutsche Telekom AG</a>
<a href="#">AS2914</a>	<a href="#">NTT America, Inc.</a>
<a href="#">AS6453</a>	<a href="#">TATA COMMUNICATIONS (AMERICA) INC</a>
<a href="#">AS3491</a>	<a href="#">PCCW Global</a>
<a href="#">AS9002</a>	<a href="#">RETN Limited</a>
<a href="#">AS37468</a>	<a href="#">Angola Cables</a>



### SUBDOMAINFINDER WEBSITE:

MOST USE THREE SOME DOMAINS ARE GIVEN BELOW:

Subdomain	IP	Cloudflare
m.wikipedia.org	185.15.59.224	
store.wikipedia.org	185.15.59.224	
zero.wikipedia.org	185.15.59.224	
IP		Count
185.15.59.224		3

### 3)SHODAN WEBSITE:

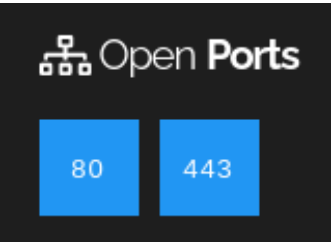
#### General Information

mediawiki.org      W.wiki      wikibooks.org.      wikidata.org  
wikifunctions.org      wikimedia.org      text-lb.eqsin.wikimedia.org  
wikimediafoundation.org

#### Hostnames

wikinews.org      wikipedia.org      wikiquote.org      wikisource.org  
wikiversity.org      wikivoyage.org      wiktioary.org      wmfusercontent.org

Country: Singapore      City: Singapore      ASN: AS14907  
Organization: Wikimedia Foundation, Inc.      ISP: Wikimedia Foundation Inc.



```
// 80 / TCP ↗

HTTP/1.1 301 Moved Permanently
content-length: 0
location: https://103.102.166.224/
server: HAProxy
x-cache: cp5019 int
x-cache-status: int-tls
connection: close
```

```
// 443 / TCP ↗ 1118261770 | 2024-07-26T23:27:22.265040

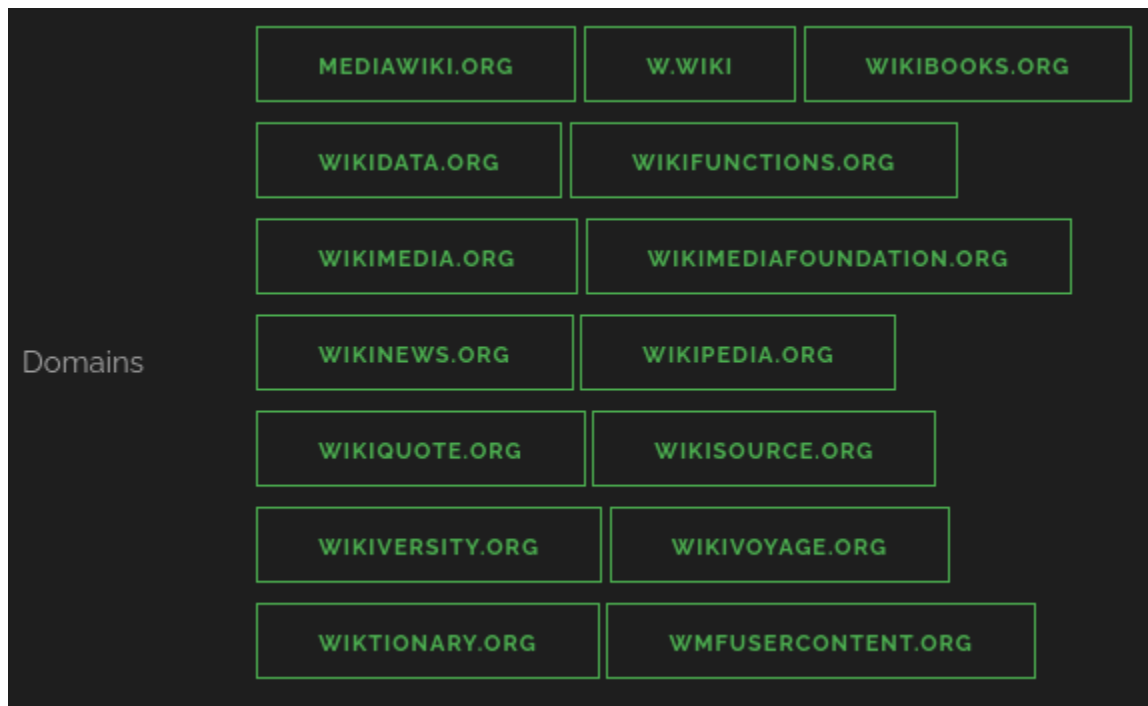
Wikimedia Error

HTTP/1.1 400
date: Fri, 26 Jul 2024 23:27:22 GMT
server: Varnish
x-cache: cp5018 int
x-cache-status: int-front
server-timing: cache;desc="int-front", host;desc="cp5018"
set-cookie: WMF-Last-Access=26-Jul-2024;Path=/;HttpOnly;secure;Expires=Tue, 27 Aug 2024 12:00:00 GMT
set-cookie: WMF-Last-Access-Global=26-Jul-2024;Path=/;Domain=.invalid;HttpOnly;secure;Expires=Tue, 27 Aug 2024 12:00:00 GMT
x-client-ip: 224.193.196.94
content-type: text/html; charset=utf-8
content-length: 1900

SSL Certificate

Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      07:41:9e:39:58:3a:4c:76:cf:1e:a1:43:47:fa:5f:3a
    Signature Algorithm: ecdsa-with-SHA384
```

DOMAIN:



*(THE INFORMATION COLLECT FROM COMMANDS AND OTHER WEBSITES ARE MATCH WITH THE INFORMATION GATNER FROM SHODAN BUT I DO NOT CV BECAUSE I DON'T LOGIN IN IT)*

#### 4)MXTOOLBOX WEBSITE:

Type	Domain Name	IP Address	TTL
A	<a href="https://wikipedia.org">wikipedia.org</a>	208.80.154.224 Wikimedia Foundation Inc. (AS14907)	5 min

	Test	Result
✓	DNS Record Published	DNS Record found

THE ALL RECOMMENDED DATA FOR REPORT LIKE

1. PORTS
2. IP ADDRESSES
3. SUBDOMAINS
4. CVE NUMBER

ARE ALL HAVE IN THE REPORT.

THE END