

ATIQ-UR-REHMAN | CERTIFIED ETHICAL HACKER | July 28, 2024

INFORMATION GATHER ABOUT WIKIPEDIA.ORG

INFO FROM COMMANDS, INFO FROM DIFF WEBSITES

# INFORMATION GATHER FROM COMMANDS:

## 1)WHOIS COMMANDS:

Domain Name: wikipedia.org

Registry Domain ID: d1a549fdfc3c4dd389c3c575a889efb1-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

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:

Wkipedia.org. 5 IN A 103.102.166.224

* Name Servers:

ns0.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 ns0.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:

0 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:ed1a::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:ed1a::1 (IPAddress)

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

dyna.wikimedia.org (FQDN) --> aaaa\_record --> 2a02:ec80:300:ed1a::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:ed1a::1 (IPAddress)

ns0.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:ed1a::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: "+000000000",

# 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>

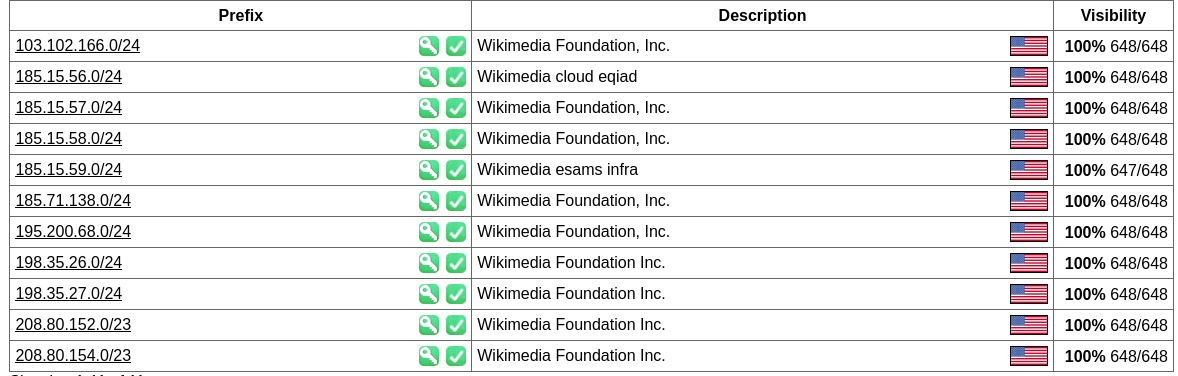
OrgTechHandle: MBE96-ARIN OrgTechName: Bergsma, Mark

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

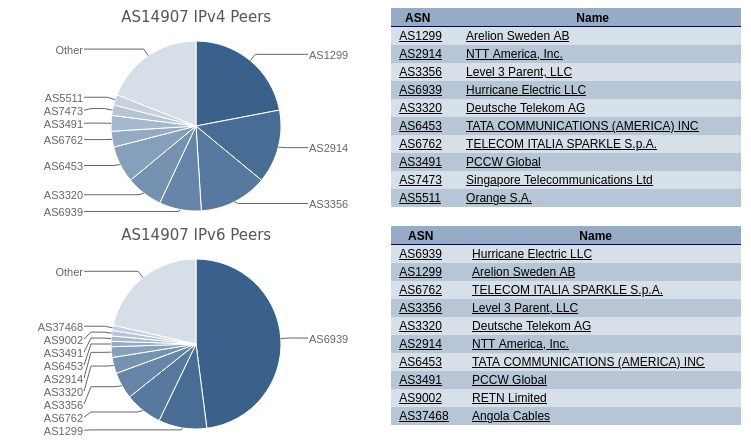
OrgTechRef: <https://rdap.arin.net/registry/entity/MBE96-ARIN>

OrgTechHandle: MOONE85-ARIN OrgTechName: Mooney, Cathal

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

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

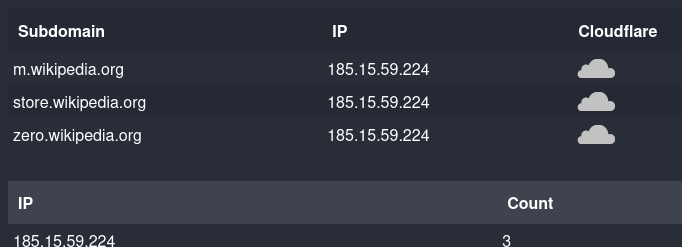
### INTERNET EXCHANGE(IE) INFO:



### AS INFORMATION

## SUBDOMAINFINDER WEBSITE:

MOST USE THREE SOME DOMAINS ARE GIVEN BELOW:



# 3)SHODAN WEBSITE:

### General Information

mediawiki.org W.wiki wikibooks.org. wikidata.org

wikifunctions.org wikimedia.org text-lb.eqsin.wikimedia.org

wikimediafoundation.org

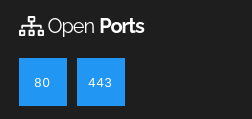
### Hostnames

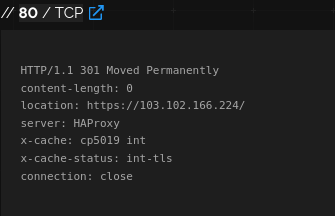
wikinews.org wikipedia.org wikiquote.org wikisource.org

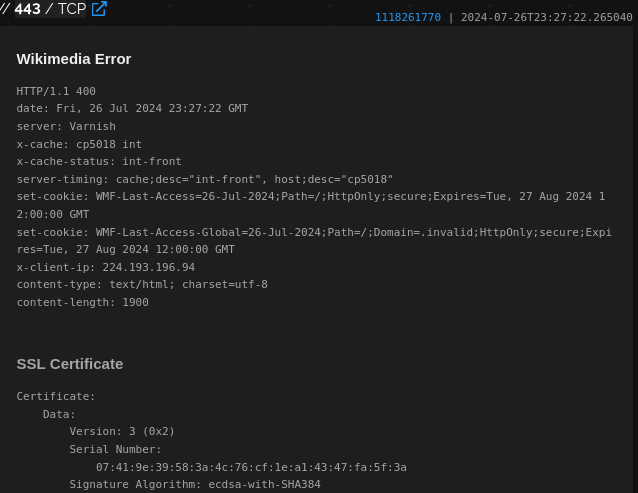
wikiversity.org wikivoyage.org wiktionary.org wmfusercontent.org

Country: Singapore City: Singapore ASN: AS14907

Organization: Wikimedia Foundation, Inc. ISP: Wikimedia Foundation Inc.







## DOMAIN:



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

## 4)MXTOOLBOX WEBSITE:

THE ALL RECOMMANDED DATA FOR REPORT LIKE

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

ARE ALL HAVE IN THE REPORT.

# THE END