DnsDumpster

DNSDumpster is a tool used for obtaining DNS information about a domain. It is a network reconnaissance tool that helps in identifying all the DNS servers and related information associated with a domain. This can be particularly useful for security professionals and researchers to understand the infrastructure of a target domain.

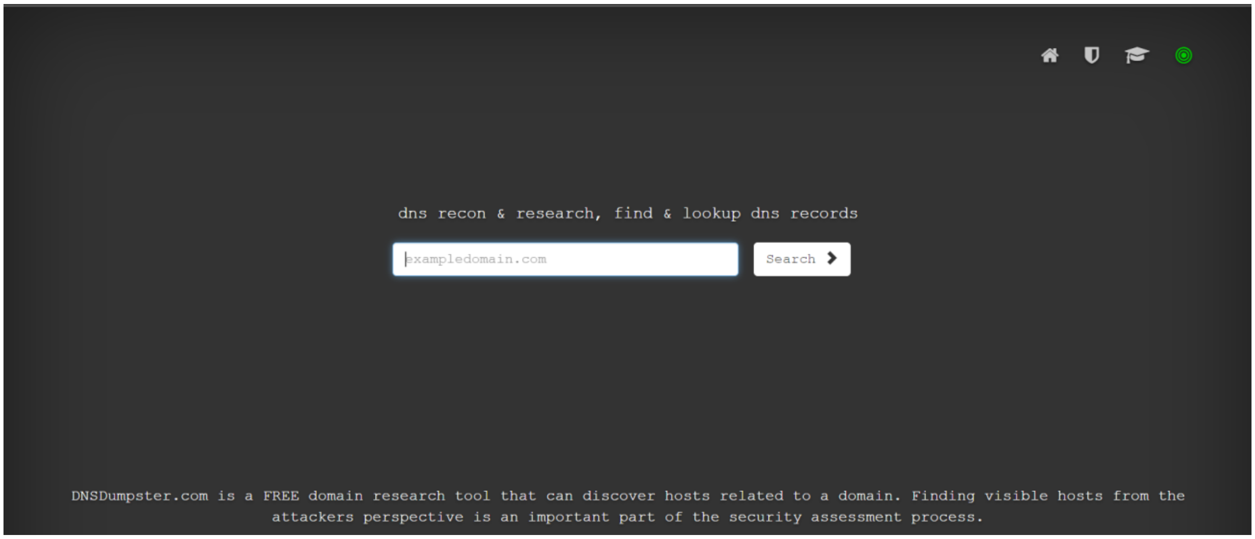
It is widely used by security professionals for gathering intelligence on a target domain during the initial phases of a penetration test or security assessment. By identifying all the publicly available assets associated with a domain, security teams can better understand the attack surface and potential vulnerabilities.

Usecase: -

- **DNS Servers: -** It is used to find the geo locations of the DNS Servers.
- **TXT Records: -** It will retrieve TXT Records of the domain.
- **MX Records: -** It is used to have insight of Mail Exchange records.
- **Host Records (A): -** It can be used to view the A records of the Domain.

Example: -

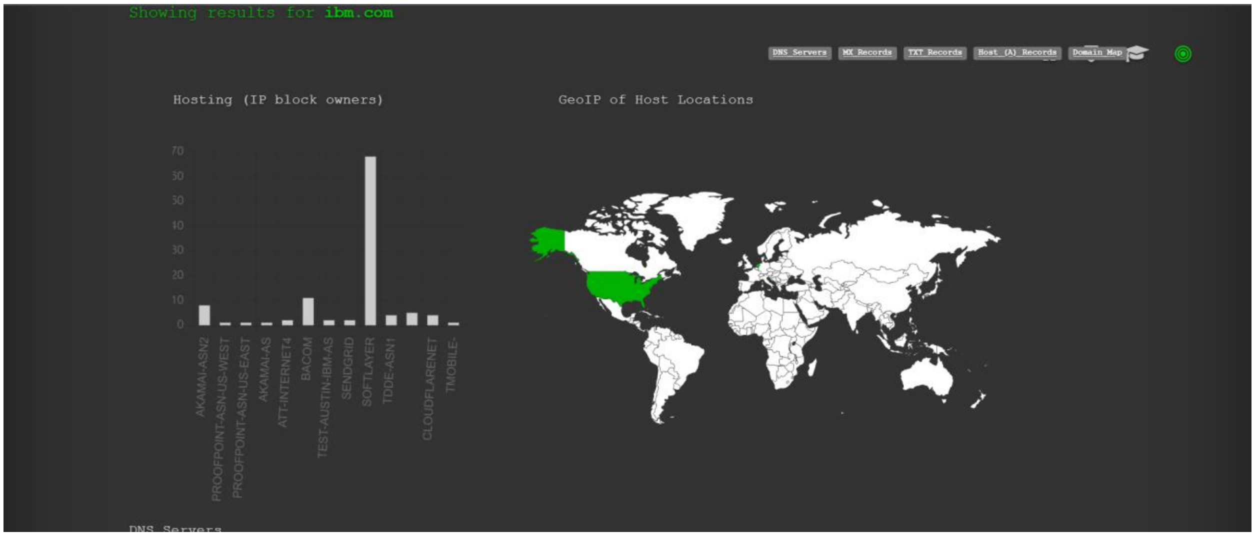
1. To have a web based insight of the information related to domain we will use the DnsDumspster.



dns recon & research, find & lookup dns records

DNSDumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

2. We will have ibm.com as our target so fill it over search bar to have information related ibm.com.



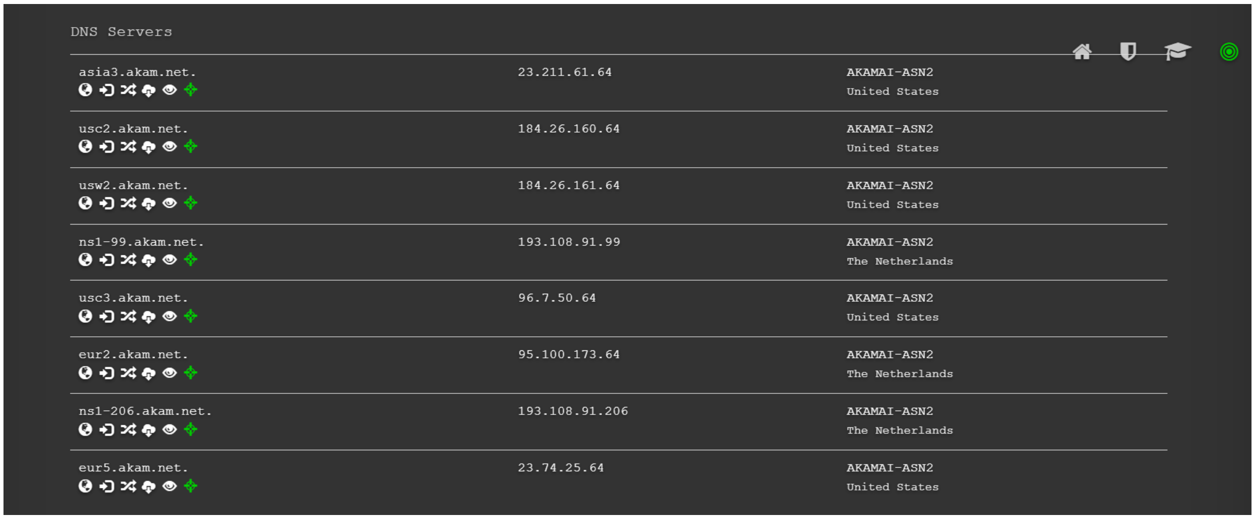
Showing results for **ibm.com**

Hosting (IP block owners)

GeoIP of Host Locations

DNS Servers

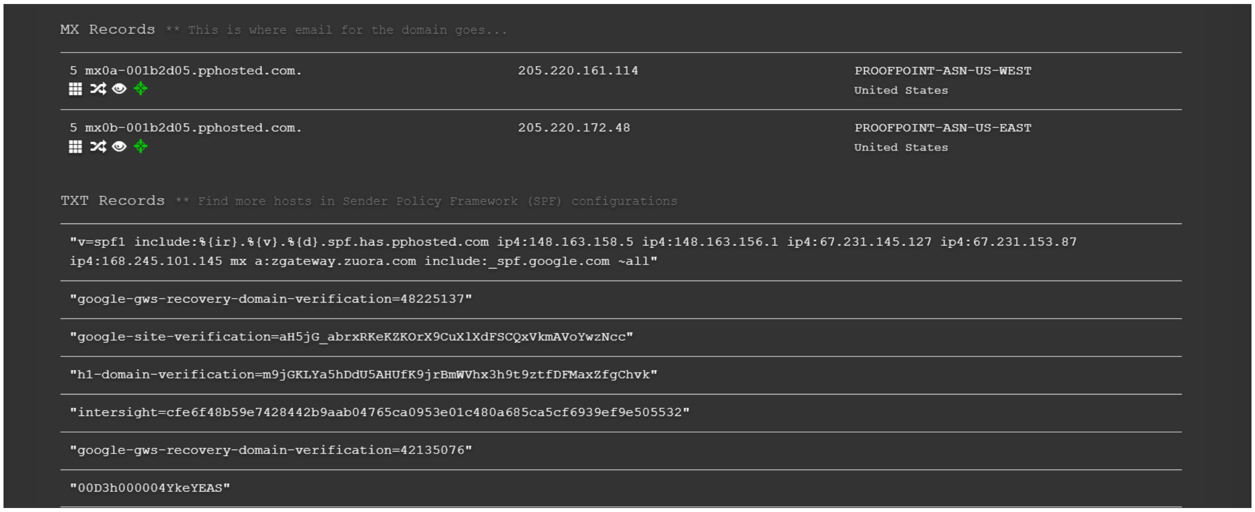
3. Firstly, we have information related to DNS servers. A DNS server translates human-readable domain names into machine-readable IP addresses, enabling devices to locate and communicate with each other on the internet. This shows the ip as well as location of the DNS servers.



DNS Servers

asia3.akam.net.	23.211.61.64	AKAMAI-ASN2 United States
usc2.akam.net.	184.26.160.64	AKAMAI-ASN2 United States
usw2.akam.net.	184.26.161.64	AKAMAI-ASN2 United States
ns1-99.akam.net.	193.108.91.99	AKAMAI-ASN2 The Netherlands
usc3.akam.net.	96.7.50.64	AKAMAI-ASN2 United States
eur2.akam.net.	95.100.173.64	AKAMAI-ASN2 The Netherlands
ns1-206.akam.net.	193.108.91.206	AKAMAI-ASN2 The Netherlands
eur5.akam.net.	23.74.25.64	AKAMAI-ASN2 United States

4. MX (Mail Exchange) records are DNS records that specify the mail servers responsible for receiving email on behalf of a domain, directing email traffic to the appropriate mail servers. This is where email for the domain goes.



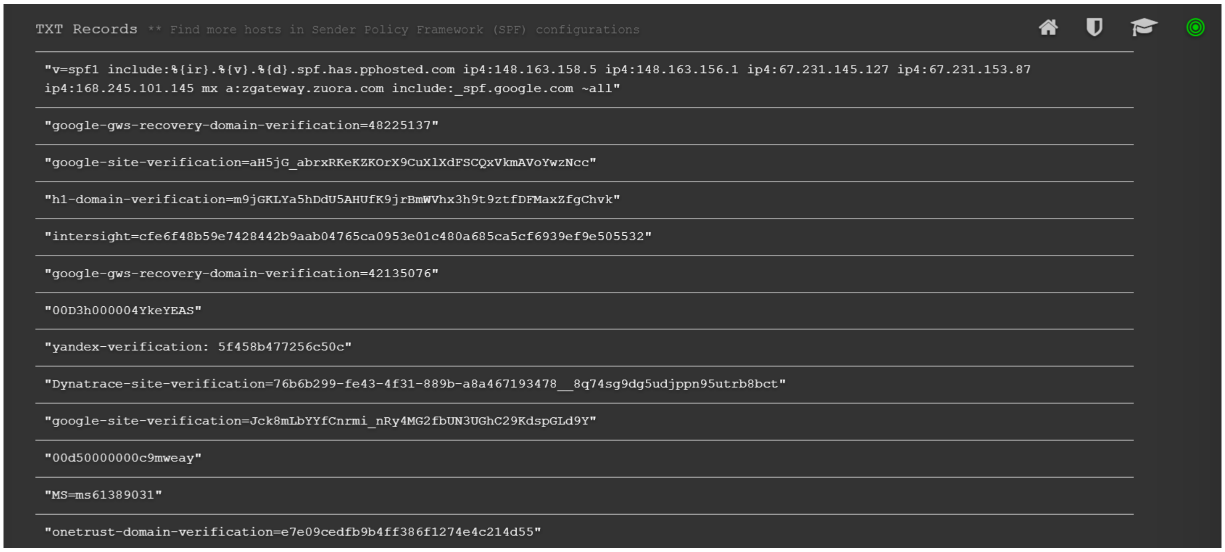
MX Records ** This is where email for the domain goes...

5 mx0a-001b2d05.pphosted.com.	205.220.161.114	PROOFPOINT-ASN-US-WEST United States
5 mx0b-001b2d05.pphosted.com.	205.220.172.48	PROOFPOINT-ASN-US-EAST United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com ip4:148.163.158.5 ip4:148.163.156.1 ip4:67.231.145.127 ip4:67.231.153.87
ip4:168.245.101.145 mx a:zgateway.zuora.com include:_spf.google.com ~all"

"google-gws-recovery-domain-verification=48225137"

"google-site-verification=aH5jG_abrxRKeKZKOrX9CuXlXdFSCQxVkmAVoYwzNcc"

"h1-domain-verification=m9jGKLYa5hDdU5AHUfK9jrBmWVhx3h9t9ztfDFMaxZfgChvk"

"intersight=cfe6f48b59e7428442b9aab04765ca0953e01c480a685ca5cf6939ef9e505532"

"google-gws-recovery-domain-verification=42135076"

"00D3h000004YkeYEAS"
```

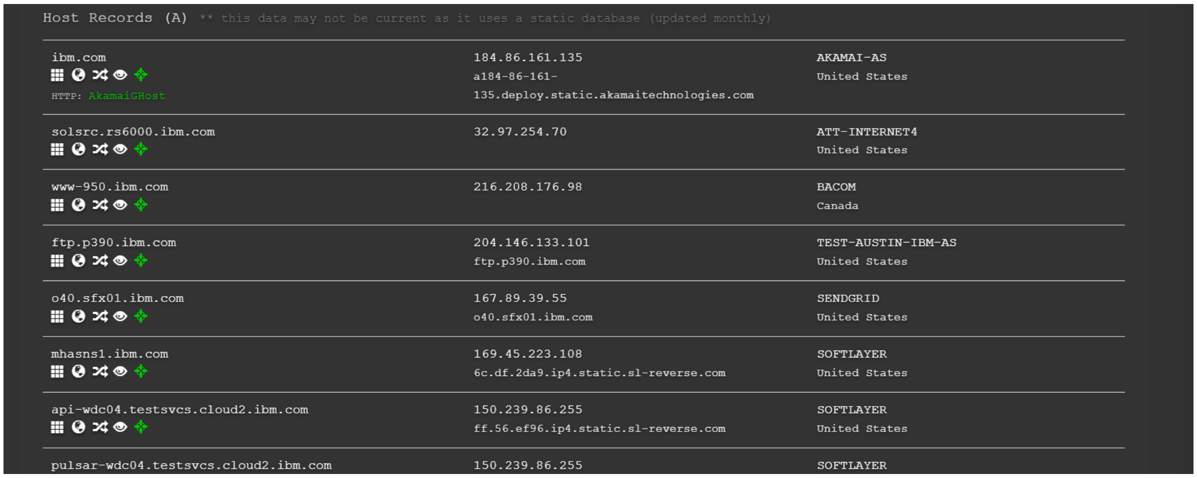
5. TXT (Text) records are DNS records that store text information related to a domain, often used for purposes such as verifying domain ownership and setting email authentication protocols like SPF, DKIM, and DMARC. It find more hosts in Sender Policy Framework (SPF) configuration.



TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

```
"v=spf1 include:%{ir}.%{v}.%{d}.spf.has.pphosted.com ip4:148.163.158.5 ip4:148.163.156.1 ip4:67.231.145.127 ip4:67.231.153.87
ip4:168.245.101.145 mx a:zgateway.zuora.com include:_spf.google.com ~all"

"google-gws-recovery-domain-verification=48225137"

"google-site-verification=aH5jG_abrxRKeKZKOrX9CuXlXdFSCQxVkmAVoYwzNcc"

"h1-domain-verification=m9jGKLYa5hDdU5AHUfK9jrBmWVhx3h9t9ztfDFMaxZfgChvk"

"intersight=cfe6f48b59e7428442b9aab04765ca0953e01c480a685ca5cf6939ef9e505532"

"google-gws-recovery-domain-verification=42135076"

"00D3h000004YkeYEAS"

"yandex-verification: 5f458b477256c50c"

"Dynatrace-site-verification=76b6b299-fe43-4f31-889b-a8a467193478__8q74sg9dg5udjppn95utrb8bct"

"google-site-verification=Jck8mLbYYfCnrmi_nRy4MG2fbUN3UGhC29KdspGLd9Y"

"00d50000000c9mweay"

"MS=ms61389031"

"onetrust-domain-verification=e7e09cedfb9b4ff386f1274e4c214d55"
```

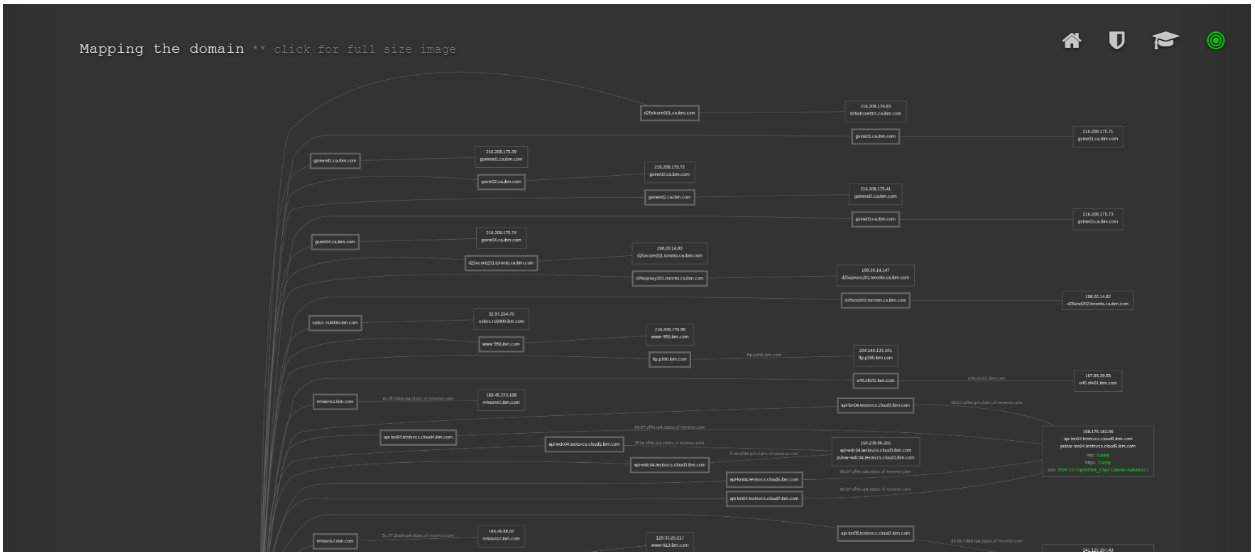
6. An A (Address) record is a DNS record that maps a domain name to its corresponding IPv4 address, allowing users to reach the website or service associated with that domain.



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

ibm.com HTTP: AkamaiGHost	184.86.161.135 a184-86-161-135.deploy.static.akamaitechnologies.com	AKAMAI-AS United States
solsrc.rs6000.ibm.com	32.97.254.70	ATT-INTERNET4 United States
www-950.ibm.com	216.208.176.98	BACOM Canada
ftp.p390.ibm.com	204.146.133.101 ftp.p390.ibm.com	TEST-AUSTIN-IBM-AS United States
o40.sfx01.ibm.com	167.89.39.55 o40.sfx01.ibm.com	SENDGRID United States
mhasns1.ibm.com	169.45.223.108 6c.df.2da9.ip4.static.sl-reverse.com	SOFTLAYER United States
api-wdc04.testsvcs.cloud2.ibm.com	150.239.86.255 ff.56.ef96.ip4.static.sl-reverse.com	SOFTLAYER United States
pulsar-wdc04.testsvcs.cloud2.ibm.com	150.239.86.255	SOFTLAYER

7. Here we have an insight of the structure of domain in a graphical tree like structure.



Mapping the domain ** click for full size image

d25xlcore001.ca.ibm.com
216.208.175.83
d25xlcore001.ca.ibm.com
gsine01.ca.ibm.com
216.208.175.71
gsine01.ca.ibm.com
gsinend1.ca.ibm.com
216.208.175.39
gsinend1.ca.ibm.com
gsine02.ca.ibm.com
216.208.175.72
gsine02.ca.ibm.com
gsinend2.ca.ibm.com
216.208.175.41
gsinend2.ca.ibm.com
gsine03.ca.ibm.com
216.208.175.73
gsine03.ca.ibm.com
gsine04.ca.ibm.com
216.208.175.74
gsine04.ca.ibm.com
d25xcore201.toronto.ca.ibm.com
198.20.14.83
d25xcore201.toronto.ca.ibm.com
d25xproxy201.toronto.ca.ibm.com
198.20.14.147
d25xproxy201.toronto.ca.ibm.com
d25xnd202.toronto.ca.ibm.com
198.20.14.82
d25xnd202.toronto.ca.ibm.com
solsrc.rs6000.ibm.com
32.97.254.70
solsrc.rs6000.ibm.com
www-950.ibm.com
216.208.176.98
www-950.ibm.com
ftp.p390.ibm.com
ftp.p390.ibm.com
204.146.133.101
ftp.p390.ibm.com
o40.sfx01.ibm.com
o40.sfx01.ibm.com
167.88.39.55
o40.sfx01.ibm.com
mhasns1.ibm.com
6c.df.2da9.ip4.static.sl-reverse.com
169.45.223.108
mhasns1.ibm.com
api-lon04.testsvcs.cloud3.ibm.com
60.b7.af9e.ip4.static.sl-reverse.com
api-lon04.testsvcs.cloud4.ibm.com
60.b7.af9e.ip4.static.sl-reverse.com
api-wdc04.testsvcs.cloud2.ibm.com
ff.56.ef96.ip4.static.sl-reverse.com
api-wdc04.testsvcs.cloud3.ibm.com
ff.56.ef96.ip4.static.sl-reverse.com
150.239.86.255
api-wdc04.testsvcs.cloud3.ibm.com
pulsar-wdc04.testsvcs.cloud3.ibm.com
158.175.183.96
api-lon04.testsvcs.cloud5.ibm.com
pulsar-lon04.testsvcs.cloud5.ibm.com
http: Caddy
https: Caddy
ssh: SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.1
api-lon04.testsvcs.cloud5.ibm.com
60.b7.af9e.ip4.static.sl-reverse.com
api-lon04.testsvcs.cloud7.ibm.com
60.b7.af9e.ip4.static.sl-reverse.com
api-lon05.testsvcs.cloud2.ibm.com
2b.6b.7d86.ip4.static.sl-reverse.com
141.125.107.43
mhasns2.ibm.com
5c.37.2ea9.ip4.static.sl-reverse.com
169.46.55.92
mhasns2.ibm.com
129.33.26.217
www-913.ibm.com