At Farsight Security, our mission is to make the internet a safer place.

During a cyber investigation, there is usually a domain or IP address that serves as your starting point. Using Farsight’s DNSDB™ – The world’s largest real-time and historical DNS Intelligence Database, there are many ways to expose the infrastructure used by cyber criminals.

7 COMMON DNSDB PIVOTS

PIVOT 01
Domain Name → IP (IPv4 A or IPv6 AAAA)
If you have a Fully Qualified Domain Name (FQDN) or base domain name, see what IP address it resolves to. You will get information for how that domain name resolves NOW, but you can also see how that name resolved over time.

PIVOT 02
IP → Domain name
If you have an IP address, either as starting original “clue” or as output from another pivot or alert, you can resolve the IP to a domain name. Farsight DNS tells us a lot more about what’s been seen so that IP address than “regular DNS” can.

PIVOT 03
IP Address → Domain names
In some cases, you may find hundreds or even thousands of domains on just a single IP. Sometimes, an entity of interest may have been given more than one IP address. If you are looking for related domains, it can be helpful to check out the entire encompassing netblock (IPv4 or IPv6). This ability to get all domain names associated with an IP address range is a very powerful passive DNS capability.

PIVOT 04
Domain → Domain names (wildcard left)
Sometimes you may know a base domain name, but you may not know the hostname/FQDN below that domain name. Look for all other hostnames/FQDNs using a wildcard on the left side.

PIVOT 05
Domain → Nameservers
If you have a domain name, see their current and previous nameservers. Then look to see what other domains also use these nameservers (see pivot 6).

PIVOT 06
Nameservers → Domains
Look to see what other domains also use those nameservers.

PIVOT 07
[hostname].* → find specified hostname in other TLDs (wildcard right)
You may be interested in seeing “variant” names exist in other Top Level Domains (TLDs) with the same starting label as a primary domain.

and many more

Learn more about DNSDB: https://www.farsightsecurity.com/solutions/dnsdb/
farsightsecurity.com
+1-650-489-7919
Copyright ©2018 Farsight Security, Inc. All rights reserved.