Navigating the Internet’s Phone Book: An Introduction to Passive DNS
Table of Contents

What Is Passive DNS? ...................................................... 3
How Passive DNS Works ...................................................... 4
Learn More ................................................................. 7
About Farsight Security ...................................................... 8
What Is Passive DNS?

Regular DNS: The “regular” Domain Name System (“DNS”) is often referred to as the Internet’s “phone book.” It resolves a symbolic domain name (such as www.farsightsecurity.com) to the IP address that computers and networks actually need (such as 104.244.14.108). The DNS usually works so well that few people think twice about it or bother to learn much about it. “It just works.”

DNS and Investigating Criminal Activity on the Internet: If you investigate cybercrimes, however, you really should be paying attention to DNS.

Why, you ask? Well, just to mention two reasons:

• Pretty much anything that happens on the Internet -- good or bad --- starts with a DNS lookup. This makes DNS a terrific way to figure out what sort of sites are getting visited. It is often easy to spot phishing web sites, sites being used to sell illegal drugs, or sites selling fake documents, for example.
• Multiple sites will often share a common web server, a common mail server, or common name servers. That means that if we can find one bad site, we can often use that initial “lead” to find additional bad sites.

Unfortunately, many of the DNS queries an investigator would LIKE to make aren’t queries that the “regular DNS” knows how to answer.

For example, you can’t ask the “regular DNS” to see all the domain names that have IP addresses from a particular network range -- the regular DNS simply doesn't know how to answer that sort of question.

Nor could you ask to see a listing of all the fully qualified domain names (“hostnames”) that exist under a particular “2nd level domain” (such as oregon.gov).

Fortunately, if you’re using passive DNS, you CAN answer those sorts of questions.
How Passive DNS Works

Passive DNS is based on passively-observed DNS queries and responses. For example, perhaps a home broadband user makes a query for www.popeyes.com, a popular (and completely legitimate) American restaurant that serves exceptionally-tasty spicy fried chicken.

Depending on where that query gets made, a passive DNS sensor may happen to see that DNS query, and see that the hostname resolves to an IP address, such as 13.52.58.70.

The passive DNS service associated with that sensor will record that information in a passive DNS database (such as Farsight’s DNSDB®).

Once that information has been added to DNSDB, DNSDB users can search DNSDB for that name, thereby learning what IP address or addresses the name has resolved to.

Users can also query for the IP address and learn the domain name that pointed at that IP.

For example, looking at the fully qualified domain name with the DNSDB command line tool dnsdbq,¹ we see:

```
$ dnsdbq -r www.popeyes.com -S -k last | more

;; record times: 2019-08-07 16:07:03 .. 2019-11-05 15:04:00

;; record times: 2017-03-31 02:33:47 .. 2019-08-07 15:59:50
[ etc ]
```

¹ [https://github.com/dnsdb/dnsdbq](https://github.com/dnsdb/dnsdbq)
In recent days (e.g., from 2019-11-05 15:04:13 to when this article was written) www.popeyes.com is a CNAME (or nickname) record, see the grey highlighted result.

That CNAME points at another domain name, note the burnt orange highlighted name (rbi.netlifyglobalcdn.com).

To find out where that domain name is actually located, we need to check passive DNS one more time:

```
$ dnsdbq -r rbi.netlifyglobalcdn.com/A -S -k last | more
;; record times: 2020-03-19 16:34:11 .. 2020-04-07 00:41:42
rbi.netlifyglobalcdn.com. A 54.156.183.85

;; record times: 2019-11-05 15:10:24 .. 2020-04-07 00:35:09
rbi.netlifyglobalcdn.com. A 35.199.169.199

;; record times: 2020-03-19 16:43:14 .. 2020-04-07 00:32:07
rbi.netlifyglobalcdn.com. A 13.52.58.70

;; record times: 2020-03-19 16:52:23 .. 2020-04-07 00:27:17
[etc]
```

Note that DNSDB reported the IP address we’d found in the “real DNS”, 13.52.58.70, but our sensors also saw other IP addresses during roughly the same time, too. In this case, because Popeyes® is a hugely popular fast food franchise, the content delivery network they’re using resolves the site’s nickname (rbi.netlifyglobalcdn.com) to multiple IP addresses during the same time period (the CDN might send queries from the West Coast of the US to one server, queries from the East Coast to another server, and queries from the Deep South to a third server). This means that we can now easily see details about this domain that we might otherwise have been hard pressed to discover.
Are there any domains that use the same CNAME? We can check by searching the “right hand side” of the records (e.g. by using -n instead of -r):

```
$ dnsdbq -n rbi.netlifyglobalcdn.com -S -k count
;; count: 179517

;; count: 29883

;; count: 28

;; count: 9
```

Well, that was unexpected! Who knew that www.timhortons.ca was related to www.popeyes.com? And what’s www.bk.com? Burger King®? Checking https://en.wikipedia.org/wiki/Restaurant_Brands_International we do indeed see that all three of those brands belong to the same fast food holding company.

Just as this sort of discovery worked for a legitimate fast food restaurant chain, it can work for illegitimate online businesses, too.
Check out these additional Passive DNS resources:

- Passive DNS for Threat Intelligence: A Technology Overview Whitepaper
  [https://info.farsightsecurity.com/passive_dns](https://info.farsightsecurity.com/passive_dns)
- Everything Starts with DNS
- A Quick Overview of the Top Seven DNS Record Types

Ready to test drive and experience how leveraging Passive DNS intelligence can accelerate your cyber investigations?

Check out Farsight’s [DNSDB® API](https://www.farsightsecurity.com/) Free 30-day Trial
About Farsight Security®

Farsight Security®, Inc. is the world's largest provider of historical and real-time DNS intelligence solutions. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security® is headquartered in San Mateo, California, USA. Learn more about how we can empower your threat platform and security team with Farsight Security® passive DNS solutions at https://www.farsightsecurity.com or follow us on Twitter: @FarsightSecInc.

To schedule a demo and obtain a free trial, contact: sales@farsightsecurity.com