FQDN to IP, IP to FQDN: The Queries that Power Domain Infrastructure Discovery

Posted on March 18, 2025

Identifying malicious infrastructure, implementing blocklists, analyzing IP or domain reputation — all of these (and many other) tasks rely on mapping fully qualified domain names (FQDNs, or so called "complete domains") to IPs and IPs to FQDNs. These mappings are crucial not only for network security analysis but also for troubleshooting and even basic website administration.

There are lookup tools that can let you obtain the IP address that resolves to the FQDN (i.e., FQDN to IP or forward lookup tools) or retrieve a list of domains resolving to an IP address (i.e., IP to FQDN also known as reverse lookup tools). If you want to dig deeper—go back in time, if you will—there are also tools that let you perform historical FQDN to IP and IP to FQDN lookups based on passive DNS data. From there, you can create a timeline of the resource's resolutions.

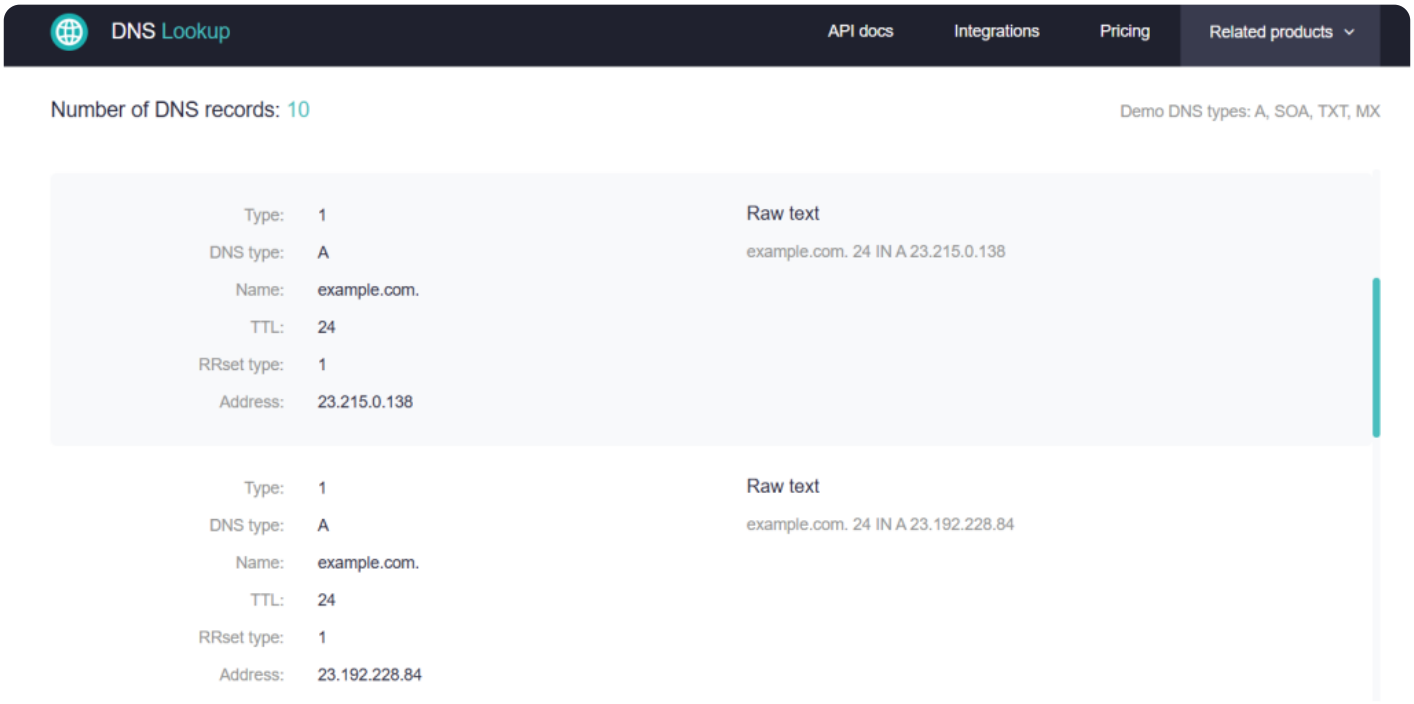
In this post, we'll show you how to do all of these. If you want to follow along and do the queries yourself, make sure to sign up for a free account to start using the tools we will be demonstrating.

Forward Lookups: Resolving a Domain to an IP Address

We begin with forward lookups, which are essentially queries where you have a domain name as a starting point.

Case 1: FQDN to IP (Current A and AAAA Records)

Let's say the domain example[.]com hypothetically caught your interest. It may have appeared multiple times on your logs, so you want to investigate it, or it may even be one of the domains you're managing and you want to verify if its DNS records are configured correctly. You can retrieve its A and AAAA records along with other DNS records using our DNS lookup tool, as shown below.



The query can be summarized in this DNS Lookup API query that you can run on your browser (you'll need to replace YOUR_API_KEY with your actual WhoisXML API key for this query to work):

https://www.whoisxmlapi.com/whoisserver/DNSService?apiKey=YOUR_API_KEY&domainName=exa

You can further limit the query to only include A records (take note of the "type" parameter at the end of the URL):

https://www.whoisxmlapi.com/whoisserver/DNSService?apiKey=YOUR_API_KEY&domainName=exa

The output looks like this:


```
<ARecord>
<type>1</type>
<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 96.7.128.175</rawText>
<address>96.7.128.175</address>
</ARecord>
<ARecord>
<type>1</type>
<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 23.192.228.84</rawText>
<address>23.192.228.84</address>
</ARecord>
<ARecord>
<type>1</type>
<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 23.215.0.138</rawText>
<address>23.215.0.138</address>
</ARecord>
<ARecord>
<type>1</type>
```

<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 23.215.0.136</rawText>
<address>23.215.0.136</address>
</ARecord>
<ARecord>
<type>1</type>
<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 96.7.128.198</rawText>
<address>96.7.128.198</address>
</ARecord>
<ARecord>
<type>1</type>
<dnsType>A</dnsType>
<name>example.com.</name>
<ttl>300</ttl>
<rRsetType>1</rRsetType>
<rawText>example.com. 300 IN A 23.192.228.80</rawText>
<address>23.192.228.80</address>
</ARecord>

It seems like there are six A records that the API fetched for example[.]com, each with a different IP address. Indeed, when you perform a DNS query, the response may include a single A record, a few, or many, depending on the domain's configuration and purpose.

What does the lookup result mean? Well, it depends primarily on whether the domain is legitimate or potentially malicious.

Both benign and malicious domains can have either one or many A or AAAA records. But it most

likely means different things.

- If there's just one DNS entry, it likely means that behind this domain there's a single server with no redundancy, used for small or internal services (e.g., personal blogs, small business sites). But it could also be a disposable malicious domain used for phishing, malware delivery, or as a basic command & control (C2) server. In the latter case, the domain would likely be relatively newly registered (which you can check using a WHOIS lookup) and may be associated with a known malicious IP. These indicators do not guarantee that the FQDN is certainly malicious, but the likelihood is relatively high.

- If there's more than one A or AAAA record, that usually indicates that the website associated with this FQDN uses load balancing or redundancy for improved availability (e.g., corporate websites, SaaS platforms, small CDNs). Dozens of records are typical for content delivery networks (CDNs) or global infrastructure. Similarly, multiple records can indicate an attempt to add redundancy to malicious infrastructure or the usage of a fast-flux botnet that makes domains switch rapidly between IP addresses. If IP addresses in all those records belong to different ASNs and different providers, that's an indicator that a domain might be suspicious. You can check this with our IP geolocation API.

Case 2: FQDN to IP (Historical A and AAAA Records)

Now, what if you want to dive a little deeper? You might want to see what an FQDN has been up to in the past—at least in terms of its IP resolutions.

Let's use the same domain (example[.]com) and query it using the DNS Chronicle API. Here's how a curl command with API query would look like:

```
curl --location 'https://dns-history.whoisxmlapi.com/api/v1' \
--header 'Content-Type: application/json' \
--data '{
"apiKey": "YOUR_API_KEY",
"searchType": "forward",
"recordType": "a",
"domainName": "example.com"
```

```
}'
```

This query returned 1,916 historical DNS A and AAAA records for the domain. To be exact, the first resolution was on October 4, 2019—the domain resolved to 80 different IP addresses on that day. Here's a snippet of the output:


```
{
  "date": "2019-10-04",
  "ips": [
   {
    "ip": "0.0.0.0",
    "wildcard": null
   },
   {
    "ip": "8.25.203.30",
    "wildcard": null
   },
   {
    "ip": "68.105.28.18",
    "wildcard": null
   },
   {
    "ip": "93.184.216.34",
    "wildcard": null
   },
   {
    "ip": "146.112.43.23",
    "wildcard": null
   },
   {
    "ip": "146.112.43.26",
    "wildcard": null
   },
```

```
{
 "ip": "146.112.43.33",
 "wildcard": null
},
{
 "ip": "146.112.43.158",
 "wildcard": null
},
{
 "ip": "146.112.43.164",
 "wildcard": null
},
{
 "ip": "146.112.43.177",
 "wildcard": null
```


The most recent A record at the time of writing this article was on February 10, 2025, when it resolved to seven different IP addresses:


```
{
  "date": "2025-02-10",
  "ips": [
  {
   "ip": "104.21.16.1",
   "wildcard": false
  },
  {
   "ip": "104.21.32.1",
   "wildcard": false
  },
  {
   "ip": "104.21.48.1",
   "wildcard": false
```

```
},
{
 "ip": "104.21.64.1",
 "wildcard": false
},
{
 "ip": "104.21.80.1",
 "wildcard": false
},
{
 "ip": "104.21.96.1",
 "wildcard": false
},
{
 "ip": "104.21.112.1",
 "wildcard": false
}
```


Having thousands of A record changes may not be as far-fetched as it may sound at first—the Internet has been around for decades, after all, and example[.]com is one of the oldest domains out there.

There are several legitimate and malicious reasons behind the number of historical DNS records a domain may have. Again, this data alone does not confirm whether a domain certainly is malicious, but it can give you some clues and further steps for research.

- A few different historical records indicate that either the domain is very new or has been stably hosted on the same server without redundancy. It could just as well be a short-lived malicious domain that was either abandoned or taken down quickly. If the domain name consists of random letters, numbers, or words that don't mean anything together (so-called DGA domains), it's likely to be on the malicious side of things.

- Dozens or hundreds of historical A and AAAA records primarily reflect that the domain has

been around for a while. They also may indicate routine infrastructure updates or hosting provider changes. In the case of malicious infrastructure, that means frequent IP rotation to evade detection—often seen in botnets, scam operations, or malware distribution networks. This behavior is suspicious if the domain is newly registered.

Reverse Lookups: Finding Domains Associated with an IP Address

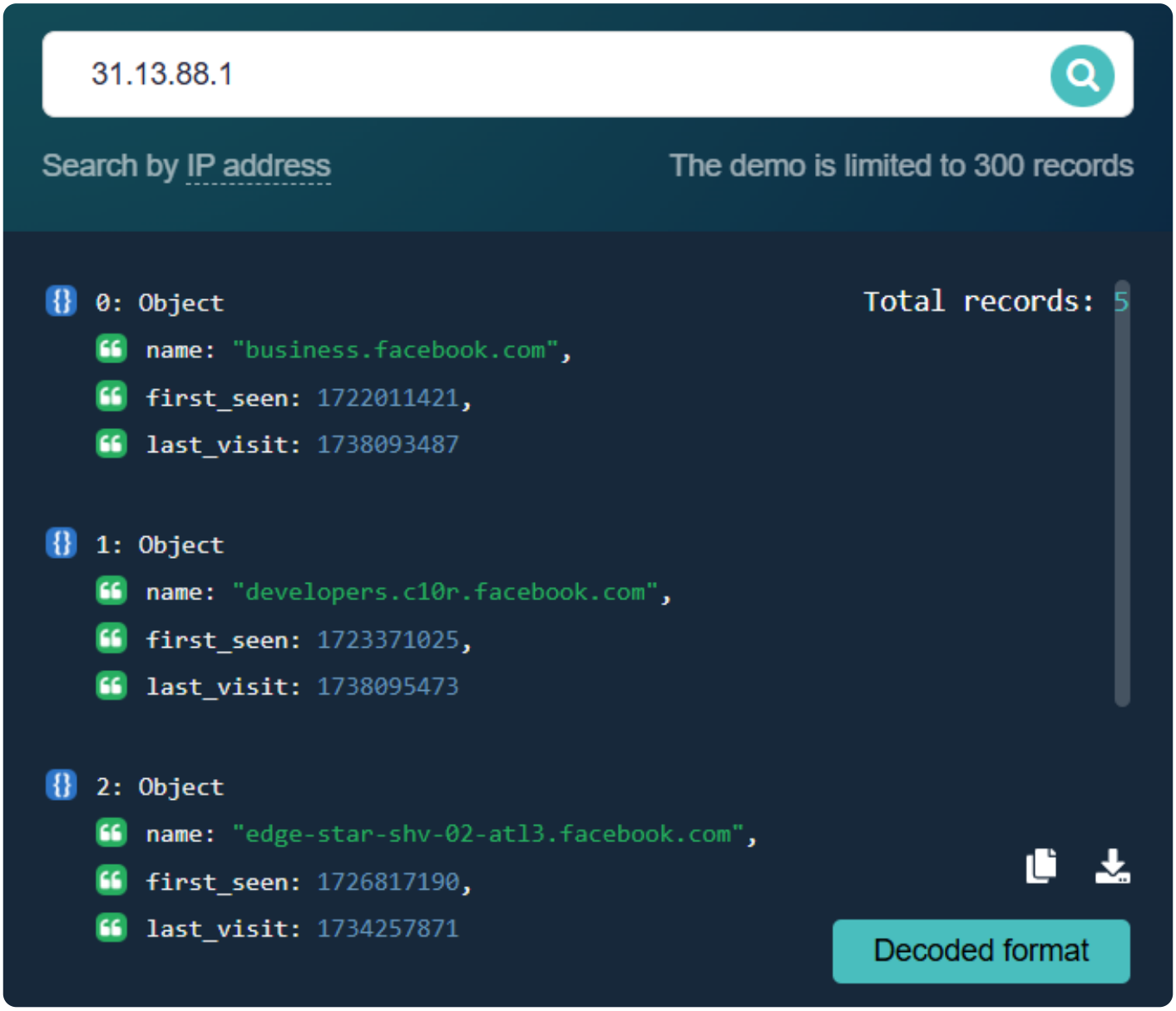
We can also go the other way around and pivot off an IP address to see the domains it is hosting and analyze its associations. This is called reverse lookups or IP to domain name lookups.

Case 3: IP to FQDN (Current Domain Connections)

Let's say you want to see all domains that currently resolve to 31.13.88.1. You can query the IP using Reverse IP API with this endpoint:

```
https://reverse-ip.whoisxmlapi.com/api/v1?apiKey=YOUR_API_KEY&ip=31.13.88.1
```

This is what it looks like on the demo page (where you can avoid writing queries and just use a Reverse IP lookup tool with a graphical user interface):



So, looking at this, we see five different FQDNs all pointing to this same IP. You also have the UNIX timestamps showing when each of those FQDNs was first and last seen.


```
[
 {
  "name": "business.facebook.com",
```

```
  "first_seen": 1722011421,
  "last_visit": 1738093487
 },
 {
  "name": "developers.c10r.facebook.com",
  "first_seen": 1723371025,
  "last_visit": 1738095473
 },
 {
  "name": "edge-star-shv-02-atl3.facebook.com",
  "first_seen": 1726817190,
  "last_visit": 1734257871
 },
 {
  "name": "star.c10r.facebook.com",
  "first_seen": 1721590130,
  "last_visit": 1740166085
 },
 {
  "name": "star.fallback.c10r.facebook.com",
  "first_seen": 1722011382,
  "last_visit": 1738095608
 }
]
```


Yet again, there are several possible interpretations for the number of connected domains an IP address may have. And again, they might indicate either a legitimate or a malicious IP address.

- Zero records usually indicate that it’s a public IP address that has not yet been used for some reason. It could also be blacklisted, abandoned, or newly acquired for future malicious use (e.g. dormant C2 infrastructure). In any case, sudden traffic from your infrastructure to an IP with zero associated domains is reason to investigate. Especially if your intrusion

detection systems indicate repeated scanning activity from such an IP address.

- One or few associated domains often indicate dedicated IP infrastructure, typically used by businesses or high-profile websites (e.g., corporate sites, SaaS platforms). Similarly, it could be dedicated IP infrastructure used for phishing, malware hosting, or single-purpose attacks (ransomware C2).

- About 50 or more associated domains indicate shared hosting, where multiple domains share an IP for cost efficiency or due to a lack of need for dedicated hosting. This type of hosting is often used by small websites (e.g., personal blogs, small businesses, early-stage startups). Malicious actors love shared hosting as well because mixing malicious domains among legitimate ones helps them hide their activity and serves as an evasion tactic. If most returned domains seem suspicious, the provider may be offering bulletproof hosting.

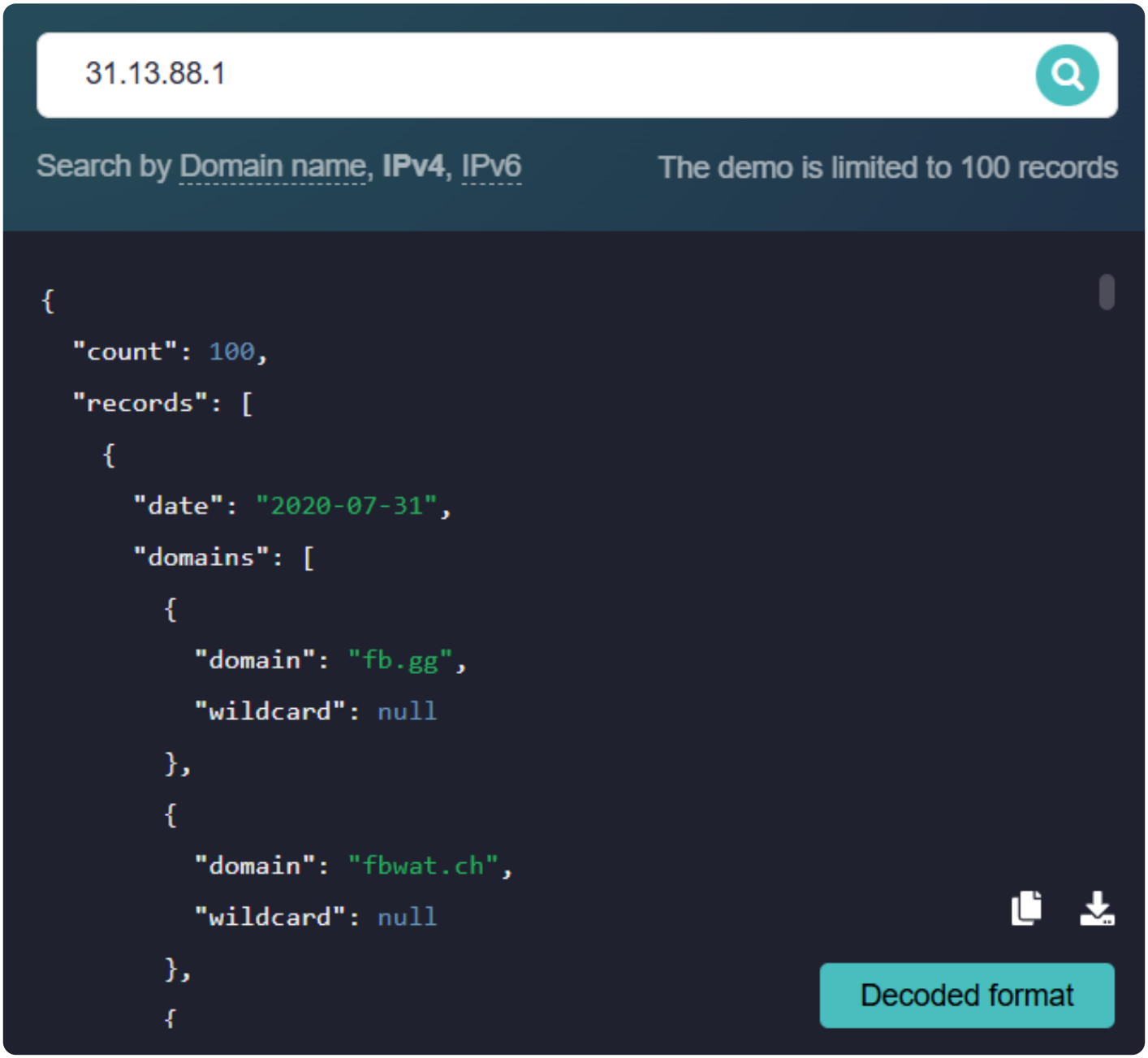
Case 4: IP to FQDN (Historical Domain Connections)

Now that you know what domains are currently connected to an IP of interest, you might want to go beyond that and see the IP's hosting history. This allows you see who else has been using the IP address over time so that you can detect suspicious associations and understand how these connections changed over time.

Let's find out all the FQDNs historically linked to 31.13.88.1—along with their timelines—using DNS Chronicle API. Here’s how that query can look like in a form of a curl command:

```
curl --location 'https://dns-history.whoisxmlapi.com/api/v1' \
    --header 'Content-Type: application/json' \
    --data '{
    "apiKey": "YOUR_API_KEY",
    "searchType": "reverse",
    "recordType": "a",
    "ipAddress": "31.13.88.1"
}'
```

Here’s what appeared on the demo page (where, again, you can just type an IP address into a GUI without dealing with shell commands).



Note that the web-based demo only returns up to 100 records. The API, on the other hand, returns 1,000 domains historically connected to the IP. The earliest domain resolution for this specific IP

was on July 31, 2020, when it resolved three domains.


```
{
 "count": 1000,
 "records": [
  {
   "date": "2020-07-31",
   "domains": [
    {
     "domain": "fb.gg",
     "wildcard": null
    },
    {
     "domain": "fbwat.ch",
     "wildcard": null
    },
    {
     "domain": "msngr.com",
     "wildcard": null
    }
   ]
  },
  {
```


Some IPs may have fewer historically connected domains, while others may have more. The logical reasons for this are quite similar to the interpretations we talked about regarding the current IP to FQDN results. However, there are some nuances.

- None or few (probably less than a hundred) historically connected domains suggest a stable IP with minimal changes, common for dedicated hosting of corporate websites and other long-standing infrastructure with low turnover. It may also indicate newly established domain

infrastructure. In the latter case, it could as well be malicious infrastructure such as a fresh phishing campaign or a C2 server that has not yet rotated domains.

- Hundreds of historically connected domains suggest shared hosting environments, where domains frequently rotate due to changes in hosting plans. It may also indicate that the IP has changed ownership, leading to a shift in the connected domain infrastructure. This shared hosting might as well be bulletproof and used primarily by malicious actors. Alternatively, they may have acquired an IP previously associated with legitimate hosting to leverage its established reputation and extend the lifespan of malicious operations. The lifespans of the domains associated with this IP could be an indicator – if most of them have existed for very short periods, that is usually a hint that they were not used for legitimate purposes.

Practical Applications of Forward and Reverse Lookup Results

You may already have a pretty good idea about what you can do with the domain-to-IP and IP-to-FQDN results. But here are a few more use cases that might be part of your security workflows.

Incident Response and Investigations

Tracking Suspicious IP Addresses

When an IP address exhibits malicious behavior (e.g., brute-force login attempts, port scanning, or appearing in a blacklist), doing a reverse lookup reveals the associated domains. This helps incident responders understand the scope of the attack, potentially even identifying and shutting down the attacker's infrastructure.

Correlating Events

Say, you received multiple security alerts involving different domains. After performing a forward

search, you discover that they all resolve to the same IP address. This may suggest a coordinated, single-purpose attack. Therefore, forward and reverse lookup queries can link different security alerts that may have otherwise been treated as separate events. As a result, you gain a more complete picture of the incident.

Threat Intelligence

Identifying Adversary-Controlled Infrastructure

Proactively monitoring IP addresses and their associated fully qualified domain names can uncover infrastructure used by threat actors for phishing, malware distribution, botnet operations, and other malicious activities. This information can be used to block access to these resources and protect users.

Predictive Threat Analysis

Analyzing historical DNS data can identify patterns and trends that might indicate future attacks. For example, a sudden increase in the registration of domains similar to a well-known company could suggest an upcoming phishing campaign.

Attack Surface Management (ASM)

Prevent Domain Hijacking and Identify DNS Misconfigurations

Regularly monitoring FQDN-to-IP mappings can help detect domain hijacking attempts early on. If a domain suddenly points to an unfamiliar IP address, it could indicate that the domain has been compromised.

Broadening the scope of forward lookups to include DNS records makes it even more comprehensive. In particular, it can help identify misconfigurations in DNS records, such as incorrect A records and dangling CNAME records.

Shadow IT Discovery

In large organizations, IP-to-domain and domain-to-IP mappings can unveil shadow IT assets. For example, a new domain that points to an internal IP address should raise a red flag, especially if it is unknown to the IT department. Someone in the organization has likely set up a service without IT approval.

Conclusion

In this post, we talked about four types of DNS lookups, namely:

- Current FQDN to IP (Forward lookup)
- Historical FQDN to IP (Forward lookup)
- Current IP to FQDN (Reverse lookup)
- Historical IP to FQDN (Reverse lookup)

These lookups can be performed using DNS Lookup API, Reverse IP API, and DNS Chronicle API , as we demonstrated throughout the article (you'll only need one API key to work with all of them).

Integrating these tools into your security workflows can add critical domain infrastructure context to your incident response, threat intelligence, ASM, threat investigations, and brand protection efforts.

Ready to map FQDNs to IPs and IPs to FQDNs? Contact us to learn how you can incorporate these processes into your workflows.