R

Reverse DNS Lookup: PTR Records, FCrDNS, Commands, and Limits

A reverse DNS lookup asks for the PTR record associated with an IP address. The IP address owner controls the reverse zone, and the returned name is not proof of identity.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

A **reverse DNS lookup (rDNS)** asks DNS for the hostname associated with an IP address . The answer is stored in a **PTR record**. This reverses the direction of a typical forward lookup, which resolves a hostname to an IPv4 A record or IPv6 AAAA record.

“Reverse lookup” can also mean a reverse phone search, reverse image search, or a service that lists domains observed on an IP. Those are different data sources. DNS rDNS answers only the PTR information published for the address.

How reverse DNS works

For IPv4, DNS reverses the address octets and queries under `in-addr.arpa`. The documentation address `192.0.2.25` becomes a query for `25.2.0.192.in-addr.arpa`. IPv6 uses reversed hexadecimal nibbles under `ip6.arpa`. The authoritative server can return one or more PTR records or no record.

The organization controlling the IP allocation normally controls or delegates the reverse zone. A website owner often cannot add a PTR record in the same DNS panel used for its domain and must request the change from the hosting provider, cloud provider, or ISP.

Forward-confirmed reverse DNS (FCrDNS)

1. Look up the IP address and obtain its PTR hostname.
2. Resolve that hostname through A or AAAA records.
3. Confirm that the original IP address appears in the forward result.

This forward confirmation detects many stale or inconsistent configurations, but it is not authentication. An IP owner that controls both directions can make them match. Use TLS, application authentication, signed email, and other evidence for trust decisions.

Commands to perform a reverse lookup

- macOS or Linux: `dig -x 192.0.2.25`
- cross-platform: `nslookup 192.0.2.25`
- Windows PowerShell: `Resolve-DnsName 192.0.2.25 -Type PTR`

Then resolve the returned hostname normally to test forward confirmation. Query a known resolver and, during troubleshooting, the authoritative server to separate cached data from zone configuration.

Common uses

- making server, firewall, and access logs easier to read;
- mail-server reputation and policy checks;
- troubleshooting DNS, service identity, and monitoring configuration;
- adding context to an IP address during an authorized investigation.

Microsoft's current reverse DNS documentation notes that PTR records and reverse zones are optional in DNS. Many residential, dynamic, shared, and privacy-addressed systems have generic PTR names or none at all.

Reverse DNS for email servers

Receiving mail systems often expect a stable PTR for the connecting IP, a sensible server hostname, and forward confirmation. Configure the server's HELO/EHLO identity consistently and also publish SPF, DKIM, and DMARC where applicable. A correct PTR supports deliverability but does not replace those controls or guarantee acceptance.

Configuration checklist

1. Choose a fully qualified hostname that has the intended A or AAAA record.
2. Request the PTR from the IP-address provider or configure it in the provider's reverse-DNS control.
3. Wait for authoritative publication and cached records to expire.
4. Test the PTR from more than one resolver and verify forward confirmation.
5. Update monitoring and mail configuration after any IP or hostname change.

Security and interpretation limits

- a PTR name is asserted by the address holder and is not verified ownership of a brand;
- cloud, CDN, proxy, VPN, and shared-hosting addresses may represent many customers;
- the absence of PTR is not proof of malicious activity;
- a previous PTR may remain cached temporarily after an update;
- do not perform blocking network lookups in a logging path without timeouts and caching.

Reverse DNS FAQ

Can I discover every domain hosted on an IP through PTR?

No. A PTR returns published reverse-DNS names, not an inventory of virtual hosts or customers.

Can a domain owner set the PTR?

Only if the reverse zone is delegated to them. Usually the ISP or hosting provider that controls the IP range must set it.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com