

NETWORK & DOMAIN LOOKUPS.



Five lookups answer almost every question about a name or an address: who is accountable for it, what it resolves to, whether packets reach it, what it presents when they do, and how it is configured. **Each one proves something narrow, and the usual mistake is reading more into it than it says.**

- REGISTRATION · RESOLUTION · REACHABILITY
- RDAP SUCCEEDS WHOIS
- A RESOLVER IS A CACHE
- ABSENCE IS NOT PROOF

01 THE MECHANISM

Registration Is a Hierarchy

IANA delegates top-level domains to registries and address blocks to the five regional registries; each publishes who holds what. RDAP returns that record as structured JSON over HTTPS, with the right server found through IANA bootstrap files. **WHOIS over port 43 is the 1980s original and still answers for many ccTLDs and every RIR.** [02] [03] [01]

Resolution Is a Cache

A recursive resolver walks root to TLD to authoritative server and keeps each answer for its TTL. What a lookup returns is that resolver's cached view at that moment, not the zone itself. **Two resolvers disagreeing is propagation, not breakage.** [04]

Everything Else Is a Connection

A traceroute, a TCP handshake, a TLS handshake and an HTTP request are things you perform, not records you read. They report what the network and the service did for *you*, from *where you asked*. **Change the vantage point and the answer can change.** [10]

02 THE FLOW

Investigate a Name INVESTIGATE

- Registration:** RDAP first for the registrable domain — registrar, creation and expiry dates, status codes and the abuse contact. A name registered days ago behind a privacy proxy is the classic phishing signature. [02]
- Resolution:** A, AAAA, MX, NS, TXT and CAA with their TTLs. NS names the DNS provider, MX names the mail path, CAA names which authorities may issue certificates for it. [04] [09]
- Presentation:** open the TLS connection and read the chain — issuer, validity window, and whether the presented names actually match the host you asked for. Then read the response headers the browser will act on. [10] [11]

Diagnose Reachability DIAGNOSE

- Classify the address:** public, private, loopback, link-local or carrier-grade NAT. A non-public address appearing as an internet source is a misconfiguration or a spoof, not a host you can reach. [06] [13]
- Connect, don't ping:** a TCP handshake to the service port separates *open* from *refused* from *filtered*. ICMP echo is widely blocked by policy, so its silence proves nothing about the service. [04]
- Trace the path:** increasing TTLs reveal each router that returns a Time Exceeded message. Read only consistent increases from a hop onward; a single slow or silent hop is usually rate-limiting.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Registration — Accountability	Who is responsible, when it was registered, when it expires, and where abuse reports go. Contact detail is largely redacted; the registrar and abuse mailbox are what stay useful.
Resolution — Mapping	What a name maps to right now, with the TTL that says how long the answer survives. Record types divide the work: addresses, mail, delegation, policy, verification.
Reachability — Path and Port	Whether packets arrive, by what route, and whether a service answers. Separating refused from filtered is the whole value; ICMP alone cannot.
Presentation — What It Shows	The certificate chain and the response headers: the identity the service claims, and the protections it asks the browser to enforce.

04 LOOKUPS COMPARED

LOOKUP	WHAT IT PROVES	WHAT IT DOES NOT
WHOIS / RDAP	Who registered the name, when, the registrar, lock status, and where abuse reports go.	Who operates it today — or, since 2018, usually any named person.
DNS query	What one resolver holds now, each record's TTL, and whether DNSSEC validated.	The authoritative zone, and anything served only on internal views.
Traceroute	Routers that answered outbound from one vantage point, and where latency rises.	The return path. A silent hop is ICMP rate-limiting, not a fault.
TCP connect	Open, refused or filtered on that port, and the handshake latency.	That the service is healthy, or that it is the one you expected.
TLS handshake	The chain presented, its validity window, and whether the names match.	The application's security. A private CA reads as untrusted from outside.
HTTP headers	What the browser is told to enforce, for one URL, at one moment.	The rest of the site, or anything the application does behind it.

NETWORK & DOMAIN LOOKUPS.

ASK · READ · VERIFY

05 READING THE OUTPUT

Read the TTL before drawing conclusions. Sixty to three hundred seconds means the answer is deliberately short-lived — a CDN, or a migration under way. A day means a change you make now stays invisible to some clients until tomorrow. Compare two resolvers rather than trusting one. [04] [05]

Separate NXDOMAIN from NODATA. The first says the name does not exist; the second says it exists with no record of that type. Different faults, and only the second is routine. [04]

Treat reverse DNS as a claim. Whoever holds the block writes the PTR. Resolve it forward and check the address comes back before using it for attribution. Mail is where its absence actually costs you. [08]

Expect redaction. Most records now show a proxy in place of a person. Work the registrar, the abuse contact and the dates instead — they stay reliable, and they are what a takedown needs. [14]

Record the vantage point. A lookup from a server is not the answer your users get; behind a CDN, the edge that answered you may not be the edge that answers them. [10]

06 SPECIFICATIONS & COVERAGE

REGISTRATION DATA

RFC 3912 defines the port-43 exchange; RFC 9083 the RDAP JSON that succeeds it, and RFC 7484 the bootstrap files that locate the right server. ICANN has required RDAP of gTLD registries since 2019. [01] [02] [03] [14]

NAME RESOLUTION

RFC 1035 defines the record types, caching and response codes; RFC 8484 carries the same queries over HTTPS. RFC 7505 gives the null MX its meaning, RFC 8659 defines CAA. [04] [05] [08] [09]

ADDRESS SPACE

RFC 6890 and the IANA special-purpose registries define which ranges are not globally routable — the list any tool checks before it connects. RFC 3021 explains the two-address /31 link. [06] [13] [07]

IDENTITY & HEADERS

RFC 6125 defines how a client matches a certificate to the name it asked for; RFC 6797 defines HSTS; OWASP Secure Headers tracks the rest. [10] [11] [12]

WHERE THIS IS EXAMINED

Network+ (resolution, record types, TTLs, addressing, path troubleshooting) · **Security+** (reconnaissance, PKI and chain of trust, hardening headers) · **CySA+** (attribution, threat intelligence) · **CCNA** (addressing, path troubleshooting) · **PenTest+** (passive footprinting).

07 WHAT THIS DOES NOT SOLVE

Redaction Hides the Person

Records name a registrar and an abuse mailbox, not a human. **Attribution needs more than a lookup.** [14]

A Resolver Is Not the Zone

You see one cache, under that provider's policy. **Internal names never appear.** [04]

One Direction, One Moment

The path is outbound from where you asked, and routes change. **The return path is invisible.**

Configuration Is Not Security

Clean headers and a valid chain remove classes of exposure. **Not the application behind them.** [12]

08 MYTHS VS. REALITY

MYTH	REALITY
“WHOIS tells you who owns a domain.”	Most records now show a proxy; the registrar, the dates and the abuse contact are the durable facts. [14]
MYTH	REALITY
“A missing PTR record is a misconfiguration.”	Most addresses never needed one. Mail servers are the exception, and there it must forward-confirm. [08]
MYTH	REALITY
“A * in a traceroute means something is broken.”	Routers rate-limit ICMP by policy. Only silence all the way to the target tells you anything.
MYTH	REALITY
“If it does not answer ping, the host is down.”	ICMP is filtered at most edges. A TCP handshake separates filtered from down.
MYTH	REALITY
“The country in an address record is where the machine is.”	It is where the block was registered ; geolocation is a separate, fuzzier question. [13]

09 SPEAK THE PROGRAM — KEY TERMS

RDAP

The structured JSON successor to WHOIS: **same data, typed fields, a defined bootstrap.** [02]

TTL

How long a resolver may keep an answer. **It sets how fast a change is seen**, not whether it is right.

NXDOMAIN VS NODATA

The name does not exist, versus **it exists with no record of that type.**

FCRDNS

A PTR name that **resolves forward to the same address.** The bar for trusting reverse DNS.

FILTERED

Silence rather than a refusal: **dropped by a firewall, or nothing is there.**

SNI

The name asked for during the handshake, **so one address can present many certificates.** [10]

SOURCES: RFC 9083 RDAP · RFC 1035 DNS · RFC 6125 SERVICE IDENTITY · OWASP SECURE HEADERS

NETWORK & DOMAIN LOOKUPS · FIELD REFERENCE