Docket

DOCKET / RESEARCH & PRACTICAL GUIDANCE

How to Verify Who Owns a Domain With RDAP (2026 Guide)

> Build a more reviewable acquisition pipeline with Docket. Our deal-origination software and managed research help private equity teams screen companies against a mandate and understand the evidence behind each finding.

Published by Docket · 2026-10-27 · how to verify who owns a domain with rdap · rdap domain ownership lookup · rdap vs whois · verify domain belongs to company · domain registrant legal entity · rdap redaction gdpr · domain ownership due diligence · entity resolution

Original article: https://docket.capital/articles/rdap-domain-ownership-verification-legal-entity



In this article

1. Executive Summary
2. Introduction and Background
3. Separating the Objects: Registrant, Registrar, Host, Operator and Entity
4. Reading a Current RDAP Record
5. Redaction, Privacy Services and Country-Code Registries
6. Reading the Website and Cross-Checking Registers
7. Shared, Delegated and Changed Domains
8. The Adjudication Worksheet, Statuses and Metrics
9. Data Analysis and Evidence
10. Case Studies and Real-World Examples
11. Implications and Future Directions
12. Frequently Asked Questions (FAQs)
13. Conclusion

Executive Summary

RDAP (Registration Data Access Protocol) is the structured, current way to read a domain's registration record, and for generic top-level domains (gTLDs) ICANN says it is now the definitive source of registration data, replacing the sunset WHOIS services from 28 January 2025 (www.icann.org). For a private-equity origination analyst the useful question is narrower than "who owns this domain". It is whether a website's claims may be attached to one specific legal entity, to a brand or parent, to several entities, or to nobody yet. RDAP is one input to that decision, and it often cannot settle it alone.

Three facts bound what an RDAP lookup can prove. First, the **ICANN Registration Data Policy**, effective 21 August 2025, requires redaction only where applicable law demands it, and lets operators but does not oblige them to consider whether data pertains to a legal person (www.icann.org). Second, redaction is signalled, not explained: a hidden registrant is an unknown, not a finding. Third, a response is a record of what a registry or registrar published, not a signed attestation of ownership; the RDAP security specification sets no current requirements for object-level integrity (www.rfc-editor.org).

Measured consistency is good but imperfect. A large-scale study found that fewer than one in ten sampled domains had inconsistent data on important fields between WHOIS and RDAP (arxiv.org), collected in December 2022 (arxiv.org), so the figure is a sample-and-period statistic and not a current error rate. Scale matters too: Verisign counted more than 400 million registrations across all TLDs at the end of Q2 2026 (investor.verisign.com), a large share of them in country-code TLDs (ccTLDs) (investor.verisign.com), where registry rules differ.

The recommended method is a crosswalk. Record the RDAP source, query time, registrant field and redaction state. Read the live site's legal disclosure (company name, register number, imprint, terms). Cross-check an official register or identifier. Treat DNS, TLS certificates, hosting and name similarity as technical links only; a domain-validated certificate vouches for control of a name, not for an organisation (letsencrypt.org). Then assign one of six dispositions: verified entity website, brand or parent relationship, shared domain, likely but

unverified, conflicting, or unknown. Two ratios keep the work honest: resolution yield (verified or explicitly related domains over eligible domains) and conflict rate (contradictory strong-source cases over reviewed domains), with unknowns reported rather than hidden.

The operating rule for research teams is simple. A domain alone never authorizes a legal-entity merge, and an unresolved identity blocks field inheritance and automated outreach until a strong source closes it. This report is entity-resolution methodology, not legal advice, and it does not describe ways to identify private individuals or bypass access controls.

Introduction and Background

A research team finds a website that says a company has 1,200 employees, three plants and a regulatory approval. The next step is to decide which record in the target database may inherit those claims. The URL is tempting evidence because it is a clean, unique string. It is not an entity identifier. A legal entity is identified by a jurisdiction plus a register number, which is how OpenCorporates keys its data (knowledge.opencorporates.com), or by a Legal Entity Identifier (LEI), a unique 20-character alphanumeric code (www.gleif.org). A domain is a name registered by someone, pointed at infrastructure run by someone else, and displaying content published by a third party.

This explainer covers how an RDAP domain lookup works, how RDAP differs from WHOIS, what redaction means after GDPR (the EU General Data Protection Regulation), how to match a registrant to a company's legal name, and what a due-diligence checklist for a domain looks like. Search results for these queries are dominated by registrars and lookup tools. One current UK tool combines the registry record, the website footer, Companies House, DNS and domain history, and labels each result by confidence (domain-checker.co.uk). What is usually missing for a private-equity workflow is the disposition step: which record may inherit the website's claims once the evidence is gathered.

Scope and limits. The article covers methodology as of October 2026. It uses primary sources: ICANN policy pages, IETF standards, registry documentation, statutes and registers, and peer-reviewed or preprint research. Two limits apply. This article does not rely on the ICANN Registration Data Lookup tool's own terms or FAQ pages. And ccTLD rules change; each registry's current page should be rechecked before a conclusion is recorded.

Separating the Objects: Registrant, Registrar, Host, Operator and Entity

Most domain-ownership errors come from collapsing distinct roles into one. Nine objects need separate columns in any worksheet.

- **Registrant (domain holder):** the party recorded as holding the registration. Under ICANN policy, the Registrant Organization entered by the holder is considered the Registered Name Holder (www.icann.org).
- **Registrar:** the company through which the name is registered. ICANN states that domain name registration is done by registrars (www.icann.org).

- **Registry:** the operator of the TLD database (for example Verisign for .com), which publishes its own RDAP service (www.verisign.com).
- **DNS operator:** whoever runs the nameservers. This is a technical role and can be a hosting company, a CDN or an agency.
- **Web host:** where the site's files or application run.
- **Website operator:** the party that publishes the content and is named in the footer, terms or imprint.
- **Brand:** a trade name or mark. A sole trader in the UK may trade under their own name or another name (www.gov.uk), and in the US several businesses can share one assumed name within a state (www.sba.gov).
- **Legal entity:** the registered person with a number in an official register.
- **Parent or target group:** the controlling entity or the set of entities the research team is screening.

The domain, the site and the legal person line up only sometimes. A parent can hold the name while a subsidiary trades on it, a case the lookup tool above states in its own words (domain-checker.co.uk). Platforms add another layer: Shopify's terms say the merchant is the seller or merchant of record (www.shopify.com), and Etsy's terms describe items as sold directly by independent sellers (www.etsy.com). Franchise systems work similarly. The US Federal Trade Commission's franchise guidance treats franchised and company-owned outlets as separate categories to disclose (www.ftc.gov), which is a neutral reminder that a location page on a brand's domain may belong to a different operator than the brand owner.

Two corollaries follow. A registrar change is not a registrant change: ICANN describes moving a name to another registrant as a separate change-of-registrant request made through the current registrar (www.icann.org). And a domain name need not match the legal business name, trademark or assumed name; the US Small Business Administration says so directly (www.sba.gov). Name similarity is therefore a retrieval hint, never a match key.

Reading a Current RDAP Record

RDAP vs WHOIS: what changed and what did not

ICANN lists RDAP's advantages over WHOIS as support for internationalization, secure access to data and differentiated access to registration data (www.icann.org). The data are not different in kind: ICANN's FAQ says the registration data is the same while the structure of the response differs (www.icann.org). The practical differences for an analyst are these.

- **Structure:** RDAP returns JSON with typed objects (domain, entity, nameserver), events, statuses, notices and remarks, where WHOIS returned free text.
- **Routing:** a WHOIS query is limited to the database queried (www.icann.org), whereas RDAP clients use the IANA bootstrap registry to find the authoritative server (www.rfc-editor.org). The bootstrap file's description line identifies it as the RDAP bootstrap file for Domain Name System registrations (data.iana.org).
- **Access control:** WHOIS has no features to control access, while RDAP lets operators vary what a requester sees by authorization. An unauthenticated client may receive no contact information (www.rfc-editor.org).

- **Status of WHOIS for gTLDs:** ICANN's user page says registries and registrars are no longer required to provide WHOIS, except for .com, .name and .post (www.icann.org). APNIC, summarising ICANN reporting, notes RDAP queries passed WHOIS queries in June 2025 (blog.apnic.net).

Because RDAP is a lookup of whatever the operator chooses to publish, its answer depends on who is asking and which server answers. A registrar's response for a domain it does not sponsor is not authoritative; ICANN's profile directs registrar services to return an HTTP 404 in that case (www.icann.org).

The field interpretation matrix

Table 1 below maps each RDAP field or role to what it supports, what is commonly redacted, the inference analysts should not draw, and the next check. Role and event definitions come from RFC 9083, the IETF standard for RDAP JSON responses.

Field or role	What it supports	Common redaction	Unsafe inference	Authority and next check
Registrant entity, organization	A candidate legal name for the holder, treated as the Registered Name Holder	A registrar may redact it if the holder does not consent to publication (www.icann.org)	That the organization is the website operator, or that a matching name is the same legal person	Policy text. Next: compare with site disclosure and an official register
Registrant name, email, phone, address	Contact route for the holder, where published	Redacted where law requires; the redacted value is omitted from output and flagged (www.icann.org)	That a blank field means a privacy service, or that a placeholder email is the holder's	Policy plus RFC 9537. Next: record as unknown, do not chase individuals
Privacy or proxy entity	The service is published as the holder of record when an affiliated or accredited service is used (www.icann.org)	Underlying customer is not shown	That the proxy is the business, or that the customer is the operating entity	Registration Data Policy. Next: rely on site and register evidence
Registration event	The date the object was initially registered (www.rfc-editor.org)	Not a personal-data field	That the domain creation date is the company's founding date	RFC 9083. Next: compare with archive first capture
Last-changed event	When information in the object last changed (www.rfc-editor.org)	Not a personal-data field	That the change was a sale	RFC 9083. Next: look for a change in site disclosure
Transfer event	Movement from one registrar to another (www.rfc-editor.org)	Not a personal-data field	That the owner changed	RFC 9083. Next: look for a change-of-registrant signal elsewhere
Registry domain and entity handles	A registry-unique object identifier (www.rfc-editor.org)	Registry IDs can be redacted under the policy	That a handle identifies a legal entity or links registrations across registrars	RFC 9083. Next: never use as an entity key

Field or role	What it supports	Common redaction	Unsafe inference	Authority and next check
Notices, remarks, redacted array	Service terms and the signal that fields were withheld (www.rfc-editor.org)	A response can say results are incomplete for lack of authorization (www.rfc-editor.org)	That the absence of a redaction flag proves nothing was withheld	RFC 9083 and RFC 9537. Next: store notices with the response

The interpretive point of *Table 1* is that RDAP rows have unequal evidential value. Only the registrant organization can support an entity hypothesis, and it is often redacted or absent. Events describe the registration object's life, not the company's. The handle is an operator-scoped identifier, and RFC 9082 adds that handle syntax is specific to the registration provider (www.rfc-editor.org), so handles cannot be compared across registries. Store the raw JSON, the server that answered, and the query time, because RFC 9537 leaves the contents of any redaction policy outside its scope (www.rfc-editor.org).

Finally, how current is the data? Registrars must validate that data elements are present and in the correct format within 15 days of registration, transfer in or update (www.icann.org). That is a format check. It is not an identity check, and Verisign's own terms for its RDAP service state that it does not guarantee accuracy (www.verisign.com).

Redaction, Privacy Services and Country-Code Registries

Interpreting redaction

RFC 9537 defines a redacted RDAP field as one that has had data removed or replaced because of server policy (www.rfc-editor.org). Under ICANN's policy, a redacted value is not output and the output must show it is redacted (www.icann.org). Holders must be offered the chance to consent to publication (www.icann.org). If a holder consents, the data appear; if not, a registrar may redact the organization. The correct reading is therefore: a missing registrant organization is an unknown, not evidence for or against anything about the registrant.

Redaction is different from a privacy or proxy service. In a proxy arrangement the provider becomes the Registered Name Holder and licenses use of the name to its customer (www.icann.org). Registrar help pages say the same in plainer language: one registrar says WHOIS can "in theory" answer who owns a domain (kb.porkbun.com) and that privacy hides the actual contact information from the public (kb.porkbun.com).

GDPR itself is narrower than many assume. The European Commission's guidance says the regulation does not govern data about companies or other legal entities (commission.europa.eu). Redaction of an organisation's name is therefore usually an operator or registry policy choice, not a legal necessity, and ICANN's policy leaves legal-person differentiation optional. In the EU, NIS2 (Directive 2022/2555) Article 28 pushes the other way by requiring access for legitimate access seekers; Article 28(5) requires Member States to make registries and registration service providers reply to access requests without undue delay and in any event within 72 hours, as Germany's reply on the European Commission's notification system quotes (a reply duty, not a promise of disclosure) (technical-regulation-information-system.ec.europa.eu), and ENISA summarises the duty to hold accurate and complete data (www.enisa.europa.eu). Access for a legitimate

seeker is a request path, not a public field. ICANN's equivalent for gTLDs is the Registration Data Request Service, a standardized format for requesting nonpublic data (www.icann.org), and a request is not a promise of disclosure.

Route country-code domains to their own registry

Do not universalise gTLD behaviour. ICANN's gTLD agreements require RDAP, but ccTLDs are not under that requirement; the preprint measured ccTLD RDAP adoption at only 9% in the IANA bootstrap file during its study period (arxiv.org), while an APNIC post of February 2026 reported about 60% of ccTLDs had deployed RDAP, counting servers outside the bootstrap file (blog.apnic.net). Verify the applicable registry before interpreting a record. Registry statements:

- **.uk (Nominet):** the .uk WHOIS is described as end of life and being phased out (registrars.nominet.uk), and Nominet offers RDAP for the TLDs it operates (registrars.nominet.uk). Its registrar documentation says name and contact details are shown only where the registrant has given permission (registrars.nominet.uk).
- **.de (DENIC):** DENIC says it publishes data relating to legal entities (ORG handles) (denic.de), flags that the legal-entity classification is indicated by the provider (denic.de), and also states that holder data is not publicly visible to third parties (denic.de). The page therefore needs a channel-by-channel test; the separate RDAP page was labelled a test operation and is undated.
- **.nl (SIDN):** for a business registrant, the registrant information is available to everyone, according to SIDN's privacy policy for Whois (www.sidn.nl).
- **.fr (Afnic):** the 2023 publication policy publishes a legal-entity holder's trading name, postal address and phone (www.afnic.fr), and lists automatable read-only access via an RDAP API (www.afnic.fr).
- **.ca (CIRA):** the name of non-individual registrants such as corporations is displayed by default (www.cira.ca), and every registrant must select a Canadian Presence Requirements category (www.cira.ca).
- **.au (auDA):** the RDAP output includes the legal name of the registrant entity (www.auda.org.au) and a Registrant ID such as an ACN (Australian Company Number) for a company (www.auda.org.au). Licence holders must keep an Australian Presence for the licence period (www.auda.org.au).
- **.eu (EURid):** the display for legal entities is limited to a short list of fields (eurid.eu), and eligibility depends on being established in the EU or EEA (help.eurid.eu).

The pattern is useful: where a registry publishes a legal-entity name and an official identifier (the .au case), RDAP can approach register-grade evidence. Where it publishes a name only, it is a lead. Where it publishes nothing for an organization, the record is unknown. Eligibility rules such as Canadian or Australian presence add only weak corroboration of a jurisdictional link.

Reading the Website and Cross-Checking Registers

Site legal disclosure

Many jurisdictions require commercial websites to display identity details, so the live site is often stronger entity evidence than RDAP. In the UK, every company must disclose specified particulars on its websites (www.legislation.gov.uk), and GOV.UK lists the company's registered office address among them (www.gov.uk). The Electronic Commerce Regulations 2002 require provider information to be easily, directly and permanently accessible (www.legislation.gov.uk) and, for a provider on a trade register, the register's details and registration number (www.legislation.gov.uk). In Germany, section 5 of the Digitale-Dienste-Gesetz requires the name and address of establishment (www.gesetze-im-internet.de) and the commercial register and number where applicable (www.gesetze-im-internet.de). The EU's Your Europe guidance tells a business website to show its legal status, legal form and any public register entry (europa.eu).

Capture these elements verbatim, with the exact page URL, the capture date and the text:

- **Legal name and legal form** (not only the brand in the header).
- **Register and registration number**, with jurisdiction.
- **Registered office or establishment address**.
- **Terms and privacy-notice entity**, which often names the contracting party and data controller.
- **Contact address and trade names** used on the site.
- **Group statements**, such as "a member of" or "operated by", recorded as statements, not as facts.

Official registers and identifiers

A register number on the site is a claim until it is checked in the register. Companies House makes all public data it holds on companies available free (www.gov.uk), but its search page is explicit that it does not check the accuracy of information filed (find-and-update.company-information.service.gov.uk). Register evidence therefore establishes that an entity exists with that name and number, not that it runs the site. GLEIF's LEI data add the official name and registered address as recorded in the official registers (www.gleif.org), and parent links are published where parents hold LEIs (www.gleif.org). As of Q2 2026, GLEIF reported the active LEI population above 3.1 million (www.gleif.org), so coverage is far from universal. The documented Level 1 elements list no website or domain field, so an LEI record cannot confirm a URL by itself.

Trademark records show a different relationship. The USPTO says the owner must be correctly identified in the application (www.uspto.gov), and a trademark owner can be a different party from the operating company. WIPO's Global Brand Database covers only trademarks from participating national and regional offices (www.wipo.int).

What technical signals do and do not prove

DNS, certificates and hosting are links between infrastructure, not ownership. Let's Encrypt does not offer Organization Validation or Extended Validation certificates (letsencrypt.org), so its certificates say nothing about the organisation. Where a certificate does carry verified subject identity, the CA/Browser Forum Baseline Requirements require the certificate authority to verify the applicant's identity (cabforum.org), which makes

organization-validated certificates a modest corroborating signal. Certificate Transparency logs are publicly auditable, append-only records of issued certificates (www.rfc-editor.org), which is useful for dating the first certificate but not for naming an owner.

Table 2 proposes evidence weights. The weights are analyst conventions for adjudication, not figures from any standard.

Evidence	Weight	Can support	Cannot support alone
Official register entry cross-referenced to the site's own stated number	Strong	Entity existence, legal name, jurisdiction, and that the site names that entity	That the entity controls the domain or the content
Site legal disclosure (imprint, footer, terms)	Strong when it carries a register number; medium without	Website operator and contracting party	That the named party holds the domain registration
RDAP registrant organization, published and consistent	Medium to strong	Domain holder of record	That the holder is the operator, or that the name matches a unique entity
Company filing or regulator or licence record naming the domain	Strong	Entity-to-domain link as declared to an authority	That the domain is current or exclusive
Parent or group statement	Medium	Brand, parent or subsidiary relationship	Which specific subsidiary operates the page
DNS, TLS, hosting, analytics tags	Weak	A technical link between sites	Ownership, control or common entity
Name similarity, shared logo or copyright line	Weak	A retrieval hypothesis	Any merge

Read *Table 2* as a hierarchy of what can close a question. Two strong, independent sources naming the same entity close it. A strong source plus a medium one supports "likely but unverified". Weak sources only generate hypotheses, and a copyright line is not independent of the site it appears on.

Shared, Delegated and Changed Domains

Shared and delegated domains

Several legitimate patterns break the one-domain-one-entity assumption. A **parent-hosted subsidiary page** sits under the parent's domain but describes another company. A **franchise or location directory** lists independently operated outlets. An **agency-held registration** is registered by a marketing firm for a client. A **marketplace profile** lives on the platform's domain and, as noted above, belongs to the seller. A **multi-entity legal notice** lists several group companies. Each is a shared-domain case, and none is automatically a problem. The adjudication question is which entity the specific page or claim belongs to, which requires page-level evidence: the imprint of that page, the terms it links to, the contracting party in its checkout.

Timelines, redirects and archives

Build a dated timeline from three sources: RDAP events, redirect behaviour and archived pages. A permanent redirect (HTTP 301) indicates the original URL's content now lives elsewhere (www.rfc-editor.org), while a 302 is temporary (www.rfc-editor.org). Neither says who owns either end. Archived captures help date a rename or migration, but the Internet Archive states that not every date for every site is complete (help.archive.org), that robots.txt blocking can exclude pages (help.archive.org), and its availability API returns just a single closest snapshot, so the CDX index is the better tool for a full capture list (archive.org). An archive gap does not show that a site was inactive.

Distinguishing a rename from a new owner or a reused domain matters because expired names can be re-registered. ICANN's registrant guidance warns that during the auto-renew period an expired name may be available to third parties for registration, depending on the registrar (www.icann.org). During the Redemption Grace Period the registry must disable DNS resolution and block transfers (www.icann.org), so a site can go dark before the name is released. Research from 2017 found about 10% of .com domains were re-registered on the same day their old registration was deleted (www.usenix.org); that measurement is dated and shows scale, not a current rate. Check whether the site disclosure and register number survive across the RDAP registration event; if the first capture after a gap shows a different legal name, treat the domain as changed hands until shown otherwise.

A registrar transfer event alone does not evidence a sale.

The Adjudication Worksheet, Statuses and Metrics

Worksheet columns

Use one row per domain, with dated, sourced cells:

- **Domain** and the exact URL examined.
- **RDAP source and query time**, including the answering server and raw JSON reference.
- **Registrant field and redaction status**: published, redacted, empty, proxy.
- **Site legal disclosure**: legal name, register number, page URL, capture date.
- **Registry or filing cross-reference**: jurisdiction, number, retrieval date.
- **Redirect target** and the status code.
- **Archive dates**: first and last captures that support the statement.
- **Relationship** to the target record.
- **Evidence** list with weights from *Table 2*.
- **Disposition** and the reviewer's reason.

Relationship graph

Record relationships as dated, sourced edges, never as attributes of a name:

- `entity_operates_site(entity, domain, source, date)`
- `entity_holds_domain(entity, domain, source, date)`
- `brand_uses_domain(brand, domain, source, date)`

- `domain_redirects_to(domain, domain, status_code, date)`

Separating `entity_holds_domain` from `entity_operates_site` encodes the registrant versus operator split. An agency-held domain yields a holds edge to the agency and an operates edge to the client, each with its own evidence.

Dispositions

- **Verified entity website:** at least two independent strong sources name the same entity as operator, and no strong source conflicts.
- **Brand or parent relationship:** the domain belongs to a brand or group, with a sourced statement tying a named entity to it; claims inherit to the brand or parent record only. For an alias or redirect of an already verified entity, the label points to that same entity record and adds no new claims.
- **Shared domain:** several entities legitimately use it; claims inherit page by page.
- **Likely but unverified:** one strong source plus corroboration; display, but do not inherit.
- **Conflicting:** strong sources disagree; hold for review and preserve both.
- **Unknown:** no usable evidence; keep visible as unknown.

Metrics

Resolution yield is verified or explicitly related domains divided by eligible domains. **Conflict rate** is contradictory strong-source cases divided by reviewed domains. Report them together with counts of likely, conflicting and unknown domains (the unresolved set), because a high yield with a hidden unknown pile is a misleading summary. Count a domain as "eligible" only if it is in scope for the review and was actually examined.

Data Analysis and Evidence

Four bodies of measurement shape how much confidence RDAP deserves.

Consistency. Fernandez and co-authors compared WHOIS and RDAP records for a sample of 55 million domain names and reported that 7.6% still presented inconsistent data on important fields such as IANA ID, creation date or nameservers (arxiv.org). The funnel started from a list of 493 million unique domain names (arxiv.org), and records were gathered between 6 and 31 December 2022 (arxiv.org). The 7.6% figure counts inconsistencies in the remaining fields after excluding email, which had the highest mismatch rates (arxiv.org). Nameserver mismatches affected only 1% of domains (arxiv.org), and where WHOIS and RDAP disagreed and DNS served as ground truth, RDAP was correct in 78% of instances examined (arxiv.org). The authors also note that no formal requirement mandates consistent results across data sources (arxiv.org). The figure is a large-sample finding for one period, not an error rate for each current lookup, and it measures consistency between two protocols, not accuracy of the registrant identity.

Redaction and privacy. An NDSS 2021 study of passive WHOIS data found that over 60% of large providers also redacted non-EEA records, beyond those in scope of European law (www.ndss-symposium.org); the authors warn their data may be biased by the location of the resolvers that supplied it (www.ndss-symposium.org). An Interisle study of gTLD data dated January 2021 found only 13.5% of domains had an

actual registrant identified in WHOIS (www.interisle.net) and that 86.5% of registrants could not be identified once redaction and proxy services were combined (www.interisle.net). A Verisign-sponsored summary of a later Interisle study reports 58.2% of examined records were behind proxy-protection services in January 2024 compared with 29.2% in November 2020 (www.dnib.com). These studies pre-date the 2025 WHOIS sunset and the August 2025 policy and should be read as direction of travel.

Scale and churn. Verisign's Domain Name Industry Brief reported 401.6 million registrations across all TLDs at the end of Q2 2026 (investor.verisign.com), with the .com base at 166.6 million (investor.verisign.com) and ccTLDs at 148.6 million (investor.verisign.com). The same report says available data are insufficient to estimate a combined quarterly renewal percentage across ccTLDs (www.dnib.com), which is a reminder that no single public statistic describes how often ccTLD domains change hands.

Operational limits. Rate limits shape any batch design. RFC 7480 notes servers may apply rate limits (www.rfc-editor.org), and the community rdap.org redirect service publishes a limit of 10 requests in 10 seconds per client (rdap.org). That service aggregates the RDAP servers it knows from IANA registrations (rdap.org); a TLD without a bootstrap entry may have no findable server, a gap RFC 9224 acknowledges (www.rfc-editor.org). Production workflows should use a bootstrap-aware client with caching and back-off.

Case Studies and Real-World Examples

(Hypothetical Example) A multi-entity manufacturer

This fictional example uses reserved .example domains and invented companies. Exemplar Components Group is a made-up UK-headquartered manufacturer with a UK parent (Exemplar Holdings Ltd), a German subsidiary (Exemplar Precision GmbH) and a marketing agency (Placeholder Web Agency Ltd). An analyst finds five web addresses claiming capacity, certifications and headcount. All lookups are fictional and dated 12 October 2026.

Table 3 shows the worksheet after review.

Domain	RDAP source and time	Registrant field	Site legal disclosure	Redirect and archive	Relationship and evidence	Disposition
exemplar.example	Registry server, 2026-10-12	Organization redacted	Footer names Exemplar Holdings Ltd with a UK company number; register entry matches	First archive capture 2014 with the same footer name	Entity operates site; register and site match, two strong sources	**Verified entity website** (Exemplar Holdings Ltd)

Domain	RDAP source and time	Registrant field	Site legal disclosure	Redirect and archive	Relationship and evidence	Disposition
exemplar-components.example	Registry server, 2026-10-12	Organization published: Exemplar Holdings Ltd	Redirects (301) to exemplar.example	Archive shows redirect since 2021	Entity holds domain; redirect shows site relationship only	**Brand or parent relationship** (Exemplar Holdings Ltd): the published registrant organization and the redirect tie it to the verified entity at exemplar.example; the holds edge is recorded separately; because the registrant organization and the redirect target are the same already verified entity, the label applies that same entity record and no new claims are inherited
exemplar-precision.example	Registry server, 2026-10-12	Organization: Placeholder Web Agency Ltd (agency)	Imprint names Exemplar Precision GmbH with a commercial register number; register entry matches	Archive consistent since 2019	Agency holds domain; GmbH operates site	**Verified entity website** (Exemplar Precision GmbH): claims inherit to the GmbH record, not the agency; the agency's holds edge is recorded separately
exemplar-group-net.example	Registry server, 2026-10-12	Registrant fields redacted	Footer shows "A member of the Exemplar group", no entity name or number	First archive capture eight weeks ago	Only name similarity and a shared logo	**Unknown**: no usable evidence; keep visible as unknown, no inheritance, no outreach
parts.exemplar.example	Same as parent	Same as parent	Terms name a third-party platform operator as the seller	Hosted on a platform	Subdomain page whose seller differs from the group	**Shared domain**: page-level evidence required

The interpretive point is that RDAP determined none of these dispositions alone. The first domain was settled by register and footer agreement even though the registrant was redacted. The third was settled by the imprint despite an RDAP organization naming a different company. The fourth stays unknown because every source is weak. Illustrative arithmetic for a larger review of 40 eligible hypothetical domains: if 18 are verified, 7 brand or parent, 4 shared, 6 likely, 2 conflicting and 3 unknown, resolution yield is (18 + 7 + 4) / 40 = 72.5%, conflict rate is 2 / 40 = 5.0%, and 11 of 40 (27.5%) stay visibly unresolved, counting likely, conflicting and unknown domains together (6 + 2 + 3). These numbers are invented for illustration and do not describe any real review.

Why unresolved identity blocks field inheritance: if the fourth domain's headcount claim were attached to Exemplar Holdings Ltd, the target record would inherit a number whose operator is unknown. The same logic blocks automated outreach, since an email drawn from an unresolved domain may go to an unrelated party,

and outreach requires its own approval path.

Implications and Future Directions

Policy is still moving. ICANN pages carry revisions, so re-read the current Registration Data Policy at the time of any audit. ICANN's Board directed continued operation of the Registration Data Request Service for up to two additional years after the pilot concluded in November 2025 (www.icann.org). In the EU, the NIS2 duties on registries and registration providers feed national implementations, such as the German draft BSI Act provision on 72-hour replies discussed in the notified document (technical-regulation-information-system.ec.europa.eu).

Cross-registry variation will persist. ccTLDs are free to choose RDAP behaviour, and the preprint's authors attribute the low ccTLD adoption seen in their study period to the absence of a requirement (arxiv.org). Teams should maintain a per-TLD registry note and a date for the last recheck.

What not to automate. Domain-ownership research touches personal data. Do not use RDAP to identify natural persons, do not attempt to bypass access controls, and do not contact a registrant contact obtained through a lookup. A request for nonpublic data goes through a legitimate path, such as ICANN's request service, and only for a lawful purpose. This is methodology for resolving organisations, not legal advice; consult counsel on cross-border access and outreach questions.

For origination teams. The practical product of this method is a clean boundary on inheritance: the evidence, its date and the disposition travel with each claim.

Frequently Asked Questions (FAQs)

How can an analyst verify who owns a domain with RDAP? Query the authoritative server found through the IANA bootstrap, store the response and time, read the registrant entity and redaction flags, then corroborate with the site's legal disclosure and an official register before assigning a disposition.

What is the difference between RDAP and WHOIS? RDAP returns structured JSON with differentiated access, while WHOIS returned free text from one queried database. ICANN says the underlying registration data are the same, and gTLD registries and registrars have not had to provide WHOIS since 28 January 2025, except for .com, .name and .post.

Why is the registrant hidden? Redaction under ICANN policy omits the value and flags it, and organisation names can be redacted when the holder has not consented. Treat it as unknown.

Does a redacted record say anything about the holder? No. Redaction is a normal outcome of policy and law. It is a gap in evidence, not a signal about the holder.

Can a registrant be matched to a company's legal name? Only as a hypothesis. Match on jurisdiction plus register number, not a name string, and confirm with a register such as Companies House, noting that it does not check the accuracy of what is filed (find-and-update.company-information.service.gov.uk).

Does a domain creation date show when the company was founded? No. The registration event records when the domain object was initially registered (www.rfc-editor.org).

Does a registrar change show a sale? No. A transfer event records movement between registrars (www.rfc-editor.org); a change of registrant is a separate process.

What does a domain-to-company verification checklist look like? Record RDAP and its time, read the site's disclosure, cross-check the register, treat technical links as weak, build the timeline, and assign one of the six dispositions.

Can one domain belong to several entities? Yes. Platforms, franchises, agencies and groups all use shared domains legitimately; see the shared-domain section for page-level handling.

Conclusion

RDAP is the right first query and a poor last word. It gives a dated, structured view of what a registry or registrar publishes to a given requester, with redaction signalled in the response. It cannot, by design, prove which legal entity operates a website, and its strongest field, the registrant organization, is often withheld. The WHOIS-versus-RDAP inconsistency study is a useful reminder that even the protocol layer is imperfect, though it describes one sample and period and not today's lookups.

The reliable path is to separate registrant, registrar, host, operator, brand and entity; capture the RDAP record and the site's own legal disclosure; cross-check an official register; treat DNS, certificates and name similarity as technical links; and keep a dated timeline that tells a rename from a new owner. The output is one of six dispositions, with yield, conflict rate and unknowns reported side by side. Where identity stays unresolved, claims do not inherit and outreach does not start. A domain alone never authorizes a legal-entity merge.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://www.icann.org/en/announcements/details/icann-update-launching-rdap-sunsetting-whois-27-01-2025-en
2. https://www.icann.org/en/contracted-parties/consensus-policies/registration-data-policy
3. https://www.rfc-editor.org/rfc/rfc7481.html
4. https://arxiv.org/abs/2406.02046
5. https://arxiv.org/pdf/2406.02046
6. https://investor.verisign.com/news-releases/news-release-details/dnibcom-reports-internet-has-4016-million-domain-name
7. https://letsencrypt.org/docs/faq
8. https://knowledge.opencorporates.com?p=19784
9. https://www.gleif.org/en/about-lei/introducing-the-legal-entity-identifier-lei
10. https://domain-checker.co.uk/domain-owner-lookup
11. https://www.icann.org/resources/pages/about-icann-faqs-2019-02-25-en
12. https://www.verisign.com/news-insights/registration-data-access-protocol/help
13. https://www.gov.uk/set-up-sole-trader/choose-your-business-name
14. https://www.sba.gov/business-guide/launch-your-business/choose-your-business-name
15. https://www.shopify.com/legal/terms

16. https://www.etsy.com/legal/terms-of-use
17. https://www.ftc.gov/system/files/documents/plain-language/bus70-franchise-rule-compliance-guide.pdf
18. https://www.icann.org/resources/pages/name-holder-faqs-2017-10-10-en
19. https://www.icann.org/rdap
20. https://www.icann.org/resources/pages/rdap-faqs-2018-08-31-en
21. https://www.rfc-editor.org/rfc/rfc9224.html
22. https://data.iana.org/rdap/dns.json
23. https://www.icann.org/resources/pages/rdap-information-for-users-2018-08-31-en
24. https://blog.apnic.net/2026/02/10/the-current-state-of-rdap
25. https://www.icann.org/en/system/files/files/rdap-response-profile-21feb24-en.pdf
26. https://www.rfc-editor.org/rfc/rfc9083.html
27. https://www.rfc-editor.org/rfc/rfc9082.html
28. https://www.rfc-editor.org/rfc/rfc9537.html
29. https://www.icann.org/en/system/files/files/importance-domain-name-registration-data-accuracy-20oct25-en.pdf
30. https://www.verisign.com/domain-names/registration-data-access-protocol/terms-service/index.xhtml
31. https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en
32. https://kb.porkbun.com/article/65-what-is-whois
33. https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/application-gdpr_en
34. https://technical-regulation-information-system.ec.europa.eu/hr/notification/26125/message/109559/EN
35. https://www.enisa.europa.eu/sites/default/files/publications/DNS%20Identity.pdf
36. https://www.icann.org/rdrs-en
37. https://registrars.nominet.uk/uk-namespace/registration-and-domain-management/query-tools/whois
38. https://registrars.nominet.uk/rdap
39. https://registrars.nominet.uk?p=4899
40. https://denic.de/en/service/whois-service
41. https://www.sidn.nl/en/nl-domain-name/about-sidns-privacy-policy-for-nl-domain-names
42. https://www.afnic.fr/wp-media/uploads/2022/12/afnic-policy-access-data-2023-01-01.pdf
43. https://www.cira.ca/en/ca-domains/whois
44. https://www.cira.ca/en/legal-policy-and-compliance/canadian-presence-requirements
45. https://www.auda.org.au/au-domain-names/au-rules-and-policies/whois-policy-2025-11
46. https://www.auda.org.au/au-domain-names/au-rules-and-policies/au-domain-administration-rules-licensing-2
47. https://eurid.eu/en/gdpr
48. https://help.eurid.eu/hc/en-gb/articles/9731617172381-Who-can-register-a-eu-or-its-variants-in-other-scripts-domain-name
49. https://www.legislation.gov.uk/uksi/2008/495/regulation/7/made
50. https://www.gov.uk/running-a-limited-company/signs-stationery-and-promotional-material
51. https://www.legislation.gov.uk/uksi/2002/2013/regulation/6
52. https://www.gesetze-im-internet.de/ddg/__5.html

53. https://europa.eu/youreurope/business/growing/digitalising/setting-up-business-website/index_en.htm
54. https://www.gov.uk/guidance/searching-the-companies-house-register
55. https://find-and-update.company-information.service.gov.uk
56. https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-1-data-who-is-who
57. https://www.gleif.org/en/lei-data/access-and-use-lei-data/level-2-data-who-owns-whom
58. https://www.gleif.org/en/newsroom/blog/the-lei-in-numbers-q2-2026-signals-growing-regional-momentum-for-the-lei
59. https://www.uspto.gov/trademarks/basics/common-problems
60. https://www.wipo.int/en/web/global-brand-database
61. https://cabforum.org/working-groups/server/baseline-requirements/requirements
62. https://www.rfc-editor.org/rfc/rfc6962.html
63. https://www.rfc-editor.org/rfc/rfc9110.html
64. https://help.archive.org/help/using-the-wayback-machine
65. https://archive.org/help/wayback_api.php
66. https://www.icann.org/resources/pages/registrant-about-errp-2018-12-07-en
67. https://www.icann.org/resources/pages/errp-2024-02-21-en
68. https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/lauinger
69. https://www.ndss-symposium.org/wp-content/uploads/ndss2021_2A-2_23134_paper.pdf
70. https://www.interisle.net/s/ContactStudy2021-ExecutiveSummary.pdf
71. https://www.dnib.com/articles/interisle-report-examines-domain-name-contact-data-availability
72. https://www.dnib.com/media/downloads/reports/domain-name-report-Q22026.pdf
73. https://www.rfc-editor.org/rfc/rfc7480.html
74. https://rdap.org

THE PUBLISHER

About Docket

Docket provides deal-origination research software and managed research for private equity firms. We help investment teams investigate acquisition targets using structured screening criteria, retained sources and reviewable company evidence. Teams can work through a self-serve platform or use managed research, depending on how they want research delivered.

Research against a defined mandate

A useful target list needs more than company names. Docket focuses on the questions that determine whether a company fits an investment mandate, including the evidence needed to support or qualify each answer. Our research approach makes the connection between screening criteria, source material and conclusions visible to the team reviewing the work.

Triage, Scout and Audit

Docket's three named research agents perform complementary tasks. Triage resolves company identity and screens fit. Scout collects sourced answers against the mandate. Audit checks retained evidence, addresses contradictions and leaves unsupported answers visibly unresolved. This structure helps reviewers distinguish established findings from missing information and questions requiring further investigation.

Evidence that supports investment-team judgment

Our research library covers market mapping, screening criteria, private-company data, succession and ownership, source evaluation and evidence standards. These resources explain the methods and limitations behind origination research. Findings support a team's judgment; they do not establish that a company is for sale or guarantee a transaction or investment outcome.

Work with Docket

Visit Docket to explore the platform, managed research and the current contact path. Read about screening criteria, evidence standards, AI research agents and market mapping.

Public examples are illustrative unless explicitly identified otherwise. Research preparation and authorized outreach are separate activities; confidential target lists and customer outcomes should never be inferred from an educational example.

Website: https://docket.capital

This article is educational. Verify consequential medical, legal, financial, regulatory and technical decisions with appropriate professionals and the cited primary sources. Company services are described separately from the article's research findings.