# Domain History Reconstruction Worksheet

A Practical Method for Reconstructing Domain Ownership When Records Conflict

This worksheet is used to reconstruct a domain's ownership and control history when no single data source is authoritative, by synthesizing identity records (WHOIS) and infrastructure signals (DNS) across time.

### HOW TO USE THIS WORKSHEET

This worksheet is meant to be completed top to bottom while actively researching a domain.
You are not trying to "look up" ownership. You are reconstructing it across time, vendors, and signals.
Fill in what you can. Leave blanks where data does not exist. Gaps are often as informative as records.

### WHEN TO USE THIS WORKSHEET

- Different tools return conflicting domain timelines.
- WHOIS data is redacted or incomplete.
- A domain appears inactive, deleted, or repurposed.
- You need to explain *how* you reached a conclusion, not just what you found.

### RULES

- Absence of evidence is not evidence of absence. Conflicting dates across vendors are common; record the earliest and latest extremes found.
- Temporal Discipline: All observations must be recorded with a "Date Observed" and "Vendor Timestamp" where available

## Part IA: Domain Birth Facts (High-Confidence, Low Interpretation)

Purpose: Anchor the timeline. The "first record" is often the most revealing.

Common sources: Historical WHOIS platforms and registrar archives (e.g., DomainTools, WhoisXML API, Whoxy).

| Data Point | Value | Vendor | First Seen | Notes |
|---|---|---|---|---|
| **Creation Date (Earliest)** | YYYY-MM-DD | *Vendor* | YYYY-MM-DD | Oldest observed wins |
| **Registrar at Birth** | Name | *Vendor* | YYYY-MM-DD | Registrar context only |

Creation dates may reflect registry import timing rather than first active use.

### EXAMPLE

A domain shows a 2018 creation date in one vendor and 2020 in another.
Record both. The earlier date often reflects pre-privacy registration or registry import timing.
That earlier snapshot usually carries higher attribution value.

## Part IB: Early Identity Artifacts (Volatile but High Signal)

Purpose: Capture what was visible before redaction. These are artifacts. They often degrade or disappear. Time context is mandatory.

| Artifact Type | Value | Vendor | Observed Date | Notes |
|---|---|---|---|---|
| **Registrant (Pre-Privacy)** | Text | *Vendor* | YYYY-MM-DD | May be partial |
| **Admin Email** | email@ | *Vendor* | YYYY-MM-DD | Often strongest link |
| **Org / Address** | Text | *Vendor* | YYYY-MM-DD | Treat cautiously |

Partial or malformed artifacts should be recorded verbatim. Do not normalize.

## Part IC: Identity Change Signals (Interpretive)

Purpose: Detect deliberate shifts. These are behavioral signals, requiring analyst judgment.

| Signal | Observed Delta | Approx Date | Vendor | Interpretation Notes |
|---|---|---|---|---|
| **Privacy Proxy Enabled** | Y / N | *YYYY-MM* | Vendor | Default vs intentional |
| **Registrar Change** | From → To | YYYY-MM | Vendor | Bulk or isolated |
| **WHOIS Redaction Pattern** | Sudden / Gradual | YYYY-MM | Vendor | Defensive behavior<br>* Confirm whether redaction aligns with registry-wide policy change. |

## Part II: The Infrastructure Bridge (Behavioral Verification)

Ownership changes are often inferred rather than explicit. When WHOIS is redacted, infrastructure history increasingly functions as the connective tissue between fragmented ownership records.

Common sources: Passive DNS, hosting history, and infrastructure intelligence tools (e.g., SecurityTrails, Netlas, Censys).

| Signal Type | Observed Span | Range | Implication |
|---|---|---|---|
| **Nameserver (NS) History** | | | Did control shift without a WHOIS update? |
| **IP Address (A-Record) Change** | | | Does the hosting location change match a buyer profile? [Note:Is the IP behind CDN, Shared hosting, Dedicated infrastructure? ] |
| **MX Record (Mail)** | | | Who handles the email infrastructure? |
| **TLS/Certificate Org** | | | Note: Usually found in external threat tools, not standard WHOIS. |

### EXAMPLES

WHOIS shows no ownership change, but nameservers move from a shared host to a dedicated provider within a narrow window.
This often indicates a transfer of control even when registrant data appears unchanged.

**Attribution Logic** (Example from Study)

If Domain A (redacted) and Domain B (known bad actor) both resolve to the same dedicated IP address, or transition to the same specific nameserver within the same time window, this strongly suggests shared control or coordination.

This signal is most meaningful when the infrastructure is dedicated rather than shared, and when timing alignment is tight.

### SIGNAL RELIABILITY (Highest to Lowest)

- MX continuity
- Nameserver continuity
- TLS org metadata
- A-record / IP churn

## Part III: The "Ghost" Check (Persistence & Erasure)

The report found that "attempts to erase history can backfire by creating visible gaps". Only specific vendors may hold the memory of a deleted asset. “Ghost” records are fragments that persist after a domain is deleted, redacted, or scrubbed. They often survive in only one database and are easy to dismiss incorrectly.

Common sources: Web archives and long-retention DNS datasets (e.g., Wayback Machine, SecurityTrails).

| Erasure Indicator | Detected? | Details |
|---|---|---|
| **Wayback "Excluded" Message** | (Y/N) | *Implies active request to scrub content.* |
| **Ghost Record (Single Vendor)** | (Y/N) | A record found in only one database (e.g., Security Trails or Wayback). Single-vendor persistence increases confidence **only if**:<br>* Vendor is known for historical retention<br>* Record is timestamped prior to privacy enablement |
| **Broken Timeline** | (Y/N) | Does the domain "disappear" from records for a period of years? Is the gap aligned with:<br>* Privacy proxy activation?<br>* Registrar change?<br>* Hosting provider shutdown? |

### Investigator Check:

- [ ] The "Deleted Site" Protocol: If the domain resolves to nothing now, did you check Wayback Machine or Security Trails? These were the only tools to find the report's "deleted" test case. Document which tools failed before which tools succeeded.
- [ ] Vendor retention policies reviewed. Crucial for expert testimony contexts.

# Part IV: Synthesis & Confidence Scoring

Since no platform provides confidence scoring, you must assign your own based on corroboration. Confidence scoring reflects investigative likelihood, not legal proof. Treat it as a working assessment that should tighten as corroboration accumulates.

This section relies on analyst judgment informed by corroboration across sources, not any single platform output.

## HOW TO THINK ABOUT THIS SECTION

This section captures your best current explanation for who controls the domain and why.

You are not required to resolve ambiguity. You are required to document how you weighed the evidence available at the time of analysis. As new records surface, this assessment should change.

### Final Attribution Assessment:

This assessment reflects likelihood, not legal ownership.

- Primary Identity Hypothesis (Working):
- Corroborating Signals: (e.g., "Pre-privacy email matches current DNS admin")
- Confidence Level:
  - [ ] High: Identity + Infrastructure overlap.
  - [ ] Medium: Identity found, but isolated in a single vendor.
  - [ ] Low: Inferred from Infrastructure only (No WHOIS match).
  - [ ] Very Low: Speculative pattern match only. No corroboration.

## EXAMPLE

Primary Identity Hypothesis (Working): Domain is controlled by the same operator as Domain B, previously attributed to Entity X.

Corroborating Signals:
– Pre-privacy administrative email appears in early WHOIS for both domains
– Both domains transition to the same dedicated nameserver within the same week
– Certificate organization metadata matches across infrastructure scans

Confidence Level: **Medium**
Rationale: Identity signal appears in a single historical vendor, but is reinforced by multiple independent infrastructure signals.