Axiom-Infra - Receipt Field Guide

*Receipts are organized in two layers. The **envelope** is the wrapper: a summary identifier, a hash, and a timestamp. The **payload** is the receipt itself: the sealed record. Every field inside the payload is included in the cryptographic hash and signature.*
Any change to any payload field breaks the seal.

Receipt Summary[i]

receipt.claim_id Unique identifier for this sealed record.
receipt.hash Hash of the sealed receipt payload.
receipt.timestamp ISO 8601 timestamp when the receipt was sealed.

Core[ii]

claim_id *Unique identifier for this sealed record.*
node_type *Identifies which node produced this receipt.*
received_at *When the request reached Axiom-Infra servers.*
sealed_at *When the cryptographic seal was computed.*
performed_at *When the capture was executed.*
verify_url *Public address where anyone can confirm this receipt.*
tier *Service tier under which the receipt was created*

Capture Node Details[iii]

submitted_url The URL submitted for capture.
final_url The resolved URL after any redirects.
page_title Title of the page at time of capture.
screenshot_url URL of the captured screenshot.
html_url URL of the HTML snapshot.
wayback_url Wayback Machine URL for this capture, if available.
whois_page_claim_id Claim ID for the WHOIS page receipt.
links_extracted Links found on the page, grouped by domain with count.

Network Layer[iv]

http_headers HTTP response headers returned by the captured URL.
tls_certificate TLS certificate details: issuer, subject, protocol, validity dates.
dns_records DNS A records resolved at time of capture.
whois WHOIS registration data: registrar, dates, name servers, status.

Hashes[v]

receipt_hash Hash of the full sealed payload.
content_hash Hash of the captured page content.
screenshot_hash Hash of the screenshot image.
policy_hash Hash of the capture policy applied.

Cryptographic Proof[vi]

rfc3161_token Timestamp token from a trusted authority, independent of Axiom-Infra. Verifiable without Axiom-Infra.
sig_algorithm Signature algorithm used to seal this record.
sig_key_version Version of the signing key used.
sig_status Result of signature verification. The value “ok” indicates the signature passed verification.

World State Witnesses[vii]

world_state.<source_a> *Raw snapshot from a queried public source, captured at the moment of receipt creation*.
world_state.<source_b> *Raw snapshot from a second source.*
world_state.<source_c> *Raw snapshot from a third source.*

Capture Node receipt structure. Placeholder values shown.


```
{
 "receipt": {
  "claim_id": "<unique identifier>",
  "hash": "<hash value>",
  "timestamp": "<ISO 8601 UTC timestamp>"
 },
 "payload": {
  "claim_id": "<unique identifier>",
  "node_type": "axiom_capture",
  "received_at": "<ISO 8601 UTC timestamp>",
  "sealed_at": "<ISO 8601 UTC timestamp>",
  "performed_at": "<ISO 8601 UTC timestamp>",
  "submitted_url": "<URL submitted by caller>",
  "final_url": "<URL after redirects>",
  "content_hash": "<hash value>",
  "screenshot_hash": "<hash value>",
  "policy_hash": "<hash value>",
  "rfc3161_token": "<timestamp token>",
  "screenshot_url": "<URL to retrieve screenshot>",
  "html_url": "<URL to retrieve captured HTML>",
  "verify_url": "https://axiominfra.io/verify/<claim_id>",
  "links_extracted": {
   "count": "<number>",
   "by_domain": { "<domain>": ["<URL>"] }
  },
  "wayback_url": "<Wayback Machine URL or null>",
  "whois": {
   "domain": "<domain>",
   "registrar": "<registrar>",
   "creation_date": "<ISO 8601 timestamp>",
   "expiration_date": "<ISO 8601 timestamp>",
   "updated_date": "<ISO 8601 timestamp>",
   "name_servers": ["<nameserver>"],
   "registrant_name": "<name or null>",
   "registrant_org": "<org or null>",
   "registrant_country": "<country or null>",
   "status": "<domain status>",
   "privacy_protected": "<boolean>"
  },
  "whois_page_claim_id": "<claim_id of whois sub-capture>",
  "page_title": "<HTML page title>",
  "http_headers": { "<header name>": "<header value>" },
  "tls_certificate": {
   "issuer": "<issuer>",
   "subject": "<subject>",
   "valid_from": "<unix timestamp>",
   "valid_to": "<unix timestamp>",
   "protocol": "<TLS version>"
  },
  "dns_records": ["<IP address>"],
  "world_state": {
   "<source_a>": { "<witness fields>": "<values>" },
   "<source_b>": { "<witness fields>": "<values>" },
   "<source_c>": { "<witness fields>": "<values>" }
  },
  "tier": "<tier identifier>",
  "receipt_hash": "<hash value>",
  "sig_algorithm": "<algorithm identifier>",
  "sig_key_version": "<integer>",
  "sig_status": "<verification result>"
 }
}
```

[i] Receipt Summary: The envelope. Carries the receipt's identifier, hash, and timestamp.
[ii] Core: Identifiers and timestamps that locate the receipt. Which node produced it, when each stage happened, and where to verify it.
[iii] Capture Node Details: What was captured about the page. URLs, title, extracted links, and references to the screenshot, HTML, and Wayback snapshot.
[iv] Network Layer: Infrastructure observed at the moment of capture. HTTP headers, TLS certificate, DNS records, and WHOIS data.
[v] Hashes: Cryptographic fingerprints of the captured content, screenshot, applied policy, and full sealed payload.
[vi] Cryptographic Proof: The signing and timestamping artifacts that make the receipt verifiable
[vii] World State Witnesses: Snapshots from three independent public sources, selected deterministically by claim_id and sealed into the receipt hash.