Fields

- Differences from Wireshark display fields

import { DirectoryListing } from "~/components";

The Cloudflare Rules language supports different types of fields such as:

- Request fields that represent the basic properties of incoming requests, including specific fields for accessing request headers, URI components, and the request body.
- Dynamic fields that represent computed or derived values, typically related to threat intelligence about an HTTP request.
- Response fields that represent the basic properties of the received response.
- Raw fields that preserve the original request values for later evaluations.

Refer to the Fields reference for the list of available fields.

Differences from Wireshark display fields

Most fields supported by the Cloudflare Rules language use the same naming conventions as Wireshark display fields. However, there are some subtle differences between Cloudflare and Wireshark:

- Wireshark supports CIDR (Classless Inter-Domain Routing) notation for expressing IP address ranges in equality comparisons (`ip.src == 1.2.3.0/24`, for example). Cloudflare does not.
  To evaluate a range of addresses using CIDR notation, use the `in` comparison operator as in this example: `ip.src in {1.2.3.0/24 4.5.6.0/24}`.
- In Wireshark, `ssl` is a protocol field containing hundreds of other fields of various types that are available for comparison in multiple ways. However, in the Rules language `ssl` is a single Boolean field that indicates whether the connection from the client to Cloudflare is encrypted.
- The Cloudflare Rules language does not support the `slice` operator.

□□□ #2
□ □□□ □□□ 2026-11-01 04:05:32 UTC
□ □□□ □□□ 2026-11-01 04:05:34 UTC