### decodehttp

パケットからHTTPヘッダーをデコードします。

#### 構文

decodehttp

#### 説明

出力されるフィールドは以下の通りです。

* **dst\_ip**: 宛先IPアドレス（IPアドレス）
* **dst\_port**: 宛先ポート（整数）
* **host**: FQDN（完全修飾ドメイン名）形式のWebサーバー名（文字列）
* **method**: HTTPメソッド（文字列）
* **path**: リソースパス（文字列）。通常はURI（Uniform Resource Identifier）。参照: <https://tools.ietf.org/html/rfc3986>
* **rcvd**: 受信データ量（整数、単位：バイト）
* **req\_time1**: 1回目のHTTPリクエスト時刻（エポック形式の時刻）
* **req\_time2**: 2回目のHTTPリクエスト時刻（エポック形式の時刻）
* **res\_time1**: 1回目のレスポンス時刻（エポック形式の時刻）
* **res\_time2**: 2回目のレスポンス時刻（エポック形式の時刻）
* **sent**: 送信データ量（整数、単位：バイト）
* **src\_ip**: 送信元IPアドレス（IPアドレス）
* **src\_port**: 送信元ポート（整数）
* **status**: サーバーのHTTPレスポンスコード（整数）。参照: <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>

#### 使用例

任意のPCAPファイルからHTTP通信のみをデコード

pcapfile /opt/logpresso/pcap/abnormal\_traffic.pcap | decodehttp