### decodehttp

Decodes the HTTP header in the packets.

#### Syntax

decodehttp

#### Description

The output fields are as follows:

* **dst\_ip**: Destination IP address (IP address)
* **dst\_port**: Destination port (integer)
* **host**: Name of the web server in the FQDN (Fully Qualified Domain Name) format (string)
* **method**: HTTP method (string)
* **path**: Resource path (string). Typically, the URI (Uniform Resource Identifier). Refer to: <https://tools.ietf.org/html/rfc3986>
* **rcvd**: Data received by the client from the server (bytes)
* **req\_time1**: Time the HTTP request is initiated (Epoch timestamp)
* **req\_time2**: Time the HTTP request is completed (Epoch timestamp)
* **res\_time1**: Time the HTTP response is initiated (Epoch timestamp)
* **res\_time2**: Time the HTTP response is completed (Epoch timestamp)
* **sent**: Data sent by the client to the server (bytes)
* **src\_ip**: Source IP address (IP address type)
* **src\_port**: Source port (integer)
* **status**: HTTP response code of the server (ingeter). Refer to: <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>

#### Usage

Decode HTTP packets from a pcap file.

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