### decodehttp

패킷에서 HTTP 헤더를 디코딩합니다.

#### 문법

decodehttp

#### 설명

출력하는 필드는 다음과 같습니다.

* **dst\_ip**: 목적지 IP 주소(IP 주소)
* **dst\_port**: 목적지 포트(정수)
* **host**: FQDN(Fully Qualified Domain Name) 형식의 웹 서버 이름(문자열)
* **method**: HTTP 메서드(문자열)
* **path**: 리소스 경로(문자열). 일반적으로 URI(Uniform Resource Identifier). 참조: <https://tools.ietf.org/html/rfc3986>
* **rcvd**: 받은 데이터(정수, 단위: 바이트)
* **req\_time1**: 첫번째 HTTP 요청 시간(epoch 형식 시간)
* **req\_time2**: 두 번째 HTTP 요청 시간(epoch 형식 시간)
* **res\_time1**: 첫번째 응답 시간(epoch 형식 시간)
* **res\_time2**: 두 번째 응답 시간(epoch 형식 시간)
* **sent**: 보낸 데이터(정수, 단위: 바이트)
* **src\_ip**: 출발지 IP 주소(IP 주소)
* **src\_port**: 출발지 포트(정수)
* **status**: 서버의 HTTP 응답 코드(정수). 참조: <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>

#### 사용 예

임의의 PCAP 파일에서 HTTP 통신만 디코딩

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