### pcapdecode

パケットをデコードし、L4メタデータを出力します。

#### 構文

pcapdecode

#### 説明

本コマンドの出力フィールドは以下の通りです。

|  |  |  |
| --- | --- | --- |
| フィールド | 型 | 説明 |
| src\_mac | 文字列 | 送信元MACアドレス |
| dst\_mac | 文字列 | 宛先MACアドレス |
| vlan\_id | 整数 | VLAN ID |
| protocol | 文字列 | esp、icmp、tcp、udpのいずれか |
| src\_ip | IPアドレス | 送信元IPアドレス |
| src\_port | 整数 | 送信元ポート |
| dst\_ip | IPアドレス | 宛先IPアドレス |
| dst\_port | 整数 | 宛先ポート |
| payload | バイナリ | パケットペイロード |

#### 使用例

# ダウンロード: https://raw.githubusercontent.com/logpresso/dataset/main/pcap/nslookup.pcap| pcapfile /opt/logpresso/nslookup.pcap | pcapdecode