### pcapdecode

Decodes the packets and outputs layer 4 metadata fields.

#### Syntax

pcapdecode

#### Description

After running the pcapdecode command, the output fields are as follows:

|  |  |  |
| --- | --- | --- |
| Field | Type | Description |
| src\_mac | String | Source MAC address |
| dst\_mac | String | Destination MAC address |
| vlan\_id | Integer | VLAN ID |
| protocol | String | esp, icmp, tcp, or udp |
| src\_ip | IP address | Source IP address |
| src\_port | Integer | Source port |
| dst\_ip | IP address | Destination IP address |
| dst\_port | Integer | Destination port |
| payload | Binary | Packet payload |

#### Usage

# Download: https://raw.githubusercontent.com/logpresso/dataset/main/pcap/nslookup.pcap| pcapfile /opt/logpresso/nslookup.pcap | pcapdecode