### pcapdecode

패캣을 디코딩해 L4 메타데이터를 출력합니다.

#### 문법

pcapdecode

#### 설명

이 명령어의 출력 필드는 다음과 같습니다.

|  |  |  |
| --- | --- | --- |
| 필드 | 유형 | 설명 |
| src\_mac | 문자열 | 출발지 MAC 주소 |
| dst\_mac | 문자열 | 목적지 MAC 주소 |
| vlan\_id | 정수 | VLAN ID |
| protocol | 문자열 | esp, icmp, tcp, udp 중 하나 |
| src\_ip | IP 주소 | 출발지 IP 주소 |
| src\_port | 정수 | 출발지 포트 |
| dst\_ip | IP 주소 | 목적지 IP 주소 |
| dst\_port | 정수 | 목적지 포트 |
| payload | 바이너리 | 패킷 페이로드 |

#### 사용 예

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