Header fields that can be extracted from a .pcap file

L2: Data Link Layer (Ethernet)

- Destination MAC address
- Source MAC address
- EtherType (identifies the next protocol, e.g., IPv4)

L3: Network Layer (IPv4)

- IP version
- Header length (IHL)
- DSCP / ECN (traffic handling)
- Total packet length
- Identification
- Flags (fragment control)
- Fragment offset
- Time to Live (TTL)
- Protocol (e.g., ICMP)
- Header checksum
- Source IP address
- Destination IP address

L4: Control Layer (ICMP)

- Type (Echo Request / Echo Reply)
- Code
- Checksum
- Identifier
- Sequence number
- Payload (data)