Get pcap file header data

Input pcap file

allocate memory 4096B

fp = 0B

memcpy data frame header 16B and data frame into mem\_buf

set flag\_EOF

Y

N

pcap file error

根據 magic判斷input file 是否為pcap

N

Y

N

**Read length is less than 4096B**

analysis data frame header and data frame start

fp += caplen

statistic

fp += caplen

indicate ip

Y

fp += 16B

N

**uncheck \_len >= data frame header + MAC + IP + Protocol**

get destination port

get source port

code

type

ICMP

UDP

TCP

get protocol

get destination ip

get source ip

get caplen

fp –= uncheck\_len

Y

if flag\_EOF is true

**4096 – checked\_len >= 16+MAC+IP+protocol**

Jump to next data frame header

fp = fp+(caplen+16- uncheck\_len)

Y

N

mem\_buf un**check data offset <= flag\_EOF**

Output

N

Y

N