以太网包头的第6字节开始的4个连续字节为源MAC地址字段位置。下面的命令为抓取所有源MAC地址为00:00:09:0f:df:e8:e3的数据包。

 # dump sniffer packet 接口名称 "(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)" 3

filters=[(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)]

0.632650 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714159

0x0000   0009 0fcd 9f48 **0009 0fdf e8e3** 0800 4500        .....H........E.

0x0010   0028 2383 4000 7f06 6acd c0a8 762d c0a8        .(#.@...j...v-..

0x0020   7601 f440 0016 16b9 4e62 87c3 28ef 5010        v..@....Nb..(.P.

0x0030   3fa0 f88f 0000                                 ?.....

0.633263 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714383

0x0000   0009 0fcd 9f48 **0009 0fdf e8e3** 0800 4500        .....H........E.

0x0010   0028 2384 4000 7f06 6acc c0a8 762d c0a8        .(#.@...j...v-..

0x0020   7601 f440 0016 16b9 4e62 87c3 29cf 5010        v..@....Nb..).P.

0x0030   3ec0 f88f 0000                                 >.....

抓取目标MAC = 00:09:0f:cd:9f:48数据包

 # dump sniffer packet 接口名称 "(ether[0:4]=0x00090fcd) and (ether[4:2]=0x9f48)" 3

interfaces=接口名称

filters=[(ether[6:4]=0x00090fdf) and (ether[10:2]=0xe8e3)]

0.632650 192.168.118.45.62528 -> 192.168.118.1.22: ack 2277714159

0x0000   0009 0fcd 9f48 **0009 0fdf e8e3** 0800 4500        .....H........E.

0x0010   0028 2383 4000 7f06 6acd c0a8 762d c0a8        .(#.@...j...v-..

0x0020   7601 f440 0016 16b9 4e62 87c3 28ef 5010        v..@....Nb..(.P.

0x0030   3fa0 f88f 0000                                 ?.....