

网络测量第一次实验报告

实验背景

网络中的分组数据一般以pcap/pcapng的格式存储，而流的划分通常基于以下五元组：

(源IP地址、目的IP地址、源端口号、目的端口号、传输层协议)

python中的dpkt模块支持多种协议的解析，例如常见的IP、TCP、UDP、SSL等。每种协议均提供单独的类解析存储数据，处理时将原始二进制数据构造为实例化对象，调用相关的API即可获取各字段的取值。

实验目的

从给定报文中将五元组相同的数据合并到一条数据流。

实验流程

我们首先读取给定的 PCAP 文件：

```
1 f = open('test0.pcap', "rb")
2 pcap = dpkt.pcap.Reader(f)
```

为了实现组流，我们将五元组格式化后作为索引（key），MAC 源地址、目的地址和报文总长度作为值（value），构建字典。

```
1 flow_len = {}
2
3 for timestamp, buf in pcap:
4
5     eth = dpkt.ethernet.Ethernet(buf)
6     ip = eth.data
7
8     fingerprint = str(str(ip.data.sport) + "," + str(ip.data.dport) + "," +
9 str(
10     eth.type) + "," + inet_to_str(ip.src) + "," + inet_to_str(ip.dst))
11     if fingerprint in flow_len:
12         flow_len[fingerprint][2] += len(ip)
13     else:
14         flow_len[fingerprint] = [mac_addr(eth.src), mac_addr(eth.dst) ,
15 len(ip)]
```

使用字典的原因是，字典使用哈希索引，在数据量较大时能够以 $O(1)$ 的时间复杂度进行搜索，提升程序运行效率。

处理完所有数据后，我们输出结果：

```

1 print("Number of flows: " + str(len(flow_len)) + "\n")
2
3 for key, value in flow_len.items():
4     key_list = key.split(",")
5     print("IP: " + key_list[3] + ":" + key_list[0] + " -> " + key_list[4] +
6           ":" + key_list[1])
7
8     if key_list[2] == str(dpkt.ethernet.ETH_TYPE_IP):
9         print("Type: IP")
10    elif key_list[2] == str(dpkt.ethernet.ETH_TYPE_IP6):
11        print("Type: IPv6")
12
13    print("Length: " + str(value[2]))
14    print("MAC: " + value[0] + " -> " + value[1] + "\n")

```

由于题目给定 PCAP 文件中仅有 IP 和 IPv6 两种格式的流，故我们仅对这两种流做了特殊处理。

实验结果

对于 test0.pcap，结果为：

```

1  Number of flows: 6
2
3  IP: 192.168.137.227:36291 -> 31.13.82.36:443
4  Type: IP
5  Length: 41251
6  MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
7
8  IP: 31.13.82.36:443 -> 192.168.137.227:36291
9  Type: IP
10 Length: 1418273
11 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
12
13 IP: 192.168.137.227:36388 -> 31.13.68.16:443
14 Type: IP
15 Length: 5712
16 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
17
18 IP: 31.13.68.16:443 -> 192.168.137.227:43030
19 Type: IP
20 Length: 988981
21 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
22
23 IP: 192.168.137.227:43030 -> 31.13.68.16:443
24 Type: IP
25 Length: 38802
26 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
27
28 IP: 31.13.68.16:443 -> 192.168.137.227:36388
29 Type: IP
30 Length: 99120
31 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

```

共找到 6 个组流，全部为 IP 格式的报文。

对于 test1.pcap, 结果为:

```
1  Number of flows: 62
2
3  IP: 192.168.137.227:36291 -> 31.13.82.36:443
4  Type: IP
5  Length: 41251
6  MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
7
8  IP: 31.13.82.36:443 -> 192.168.137.227:36291
9  Type: IP
10 Length: 1418273
11 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
12
13 IP: 192.168.137.227:36388 -> 31.13.68.16:443
14 Type: IP
15 Length: 5712
16 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
17
18 IP: 31.13.68.16:443 -> 192.168.137.227:43030
19 Type: IP
20 Length: 988981
21 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
22
23 IP: 192.168.137.227:43030 -> 31.13.68.16:443
24 Type: IP
25 Length: 38802
26 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
27
28 IP: 31.13.68.16:443 -> 192.168.137.227:36388
29 Type: IP
30 Length: 99120
31 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
32
33 IP: 192.168.137.227:49685 -> 31.13.82.1:443
34 Type: IP
35 Length: 28167
36 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
37
38 IP: 192.168.137.227:43039 -> 31.13.68.16:443
39 Type: IP
40 Length: 4033
41 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
42
43 IP: 31.13.82.1:443 -> 192.168.137.227:49685
44 Type: IP
45 Length: 76378
46 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
47
48 IP: 31.13.68.16:443 -> 192.168.137.227:43039
49 Type: IP
50 Length: 85675
51 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
52
53 IP: 192.168.137.227:43029 -> 31.13.68.16:443
```

54 Type: IP
55 Length: 1430
56 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
57
58 IP: 31.13.82.34:443 -> 192.168.137.227:53351
59 Type: IP
60 Length: 3938
61 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
62
63 IP: 192.168.137.227:53351 -> 31.13.82.34:443
64 Type: IP
65 Length: 7246
66 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
67
68 IP: 31.13.68.16:443 -> 192.168.137.227:43029
69 Type: IP
70 Length: 8012
71 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
72
73 IP: 192.168.137.227:63282 -> 192.168.137.1:53
74 Type: IP
75 Length: 71
76 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
77
78 IP: 192.168.137.1:53 -> 192.168.137.227:63282
79 Type: IP
80 Length: 87
81 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
82
83 IP: 192.168.137.227:50262 -> 31.13.68.13:443
84 Type: IP
85 Length: 239749
86 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
87
88 IP: 192.168.137.227:40723 -> 31.13.68.13:443
89 Type: IP
90 Length: 190641
91 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
92
93 IP: 31.13.68.13:443 -> 192.168.137.227:50262
94 Type: IP
95 Length: 6860167
96 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
97
98 IP: 31.13.68.13:443 -> 192.168.137.227:40723
99 Type: IP
100 Length: 4173536
101 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
102
103 IP: 192.168.137.227:5353 -> 224.0.0.251:5353
104 Type: IP
105 Length: 1260
106 MAC: fc:db:b3:e9:37:96 -> 01:00:5e:00:00:fb
107
108 IP: 192.168.137.227:48194 -> 192.168.137.1:53

109 Type: IP
110 Length: 67
111 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
112
113 IP: 192.168.137.1:53 -> 192.168.137.227:48194
114 Type: IP
115 Length: 106
116 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
117
118 IP: 192.168.137.227:43042 -> 31.13.68.16:443
119 Type: IP
120 Length: 42571
121 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
122
123 IP: 31.13.68.16:443 -> 192.168.137.227:43042
124 Type: IP
125 Length: 1551478
126 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
127
128 IP: 192.168.137.227:43034 -> 31.13.68.16:443
129 Type: IP
130 Length: 3803
131 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
132
133 IP: 31.13.68.16:443 -> 192.168.137.227:43034
134 Type: IP
135 Length: 99268
136 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
137
138 IP: 192.168.137.227:42355 -> 192.168.137.1:53
139 Type: IP
140 Length: 75
141 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
142
143 IP: 192.168.137.1:53 -> 192.168.137.227:42355
144 Type: IP
145 Length: 142
146 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
147
148 IP: 192.168.137.227:61764 -> 192.168.137.1:53
149 Type: IP
150 Length: 86
151 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
152
153 IP: 192.168.137.1:53 -> 192.168.137.227:61764
154 Type: IP
155 Length: 86
156 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
157
158 IP: fe80::6887:ef8:5ff2:e052:546 -> ff02::1:2:547
159 Type: IPv6
160 Length: 143
161 MAC: 22:53:49:24:ae:9a -> 33:33:00:01:00:02
162
163 IP: 192.168.137.227:36857 -> 121.51.131.223:8081

164 Type: IP
165 Length: 1317
166 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
167
168 IP: 121.51.131.223:8081 -> 192.168.137.227:36857
169 Type: IP
170 Length: 412
171 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
172
173 IP: 31.13.82.1:443 -> 192.168.137.227:49686
174 Type: IP
175 Length: 221
176 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
177
178 IP: 192.168.137.227:49686 -> 31.13.82.1:443
179 Type: IP
180 Length: 239
181 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
182
183 IP: 31.13.82.36:443 -> 192.168.137.227:36282
184 Type: IP
185 Length: 181
186 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
187
188 IP: 192.168.137.227:36282 -> 31.13.82.36:443
189 Type: IP
190 Length: 104
191 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
192
193 IP: 31.13.68.16:443 -> 192.168.137.227:43031
194 Type: IP
195 Length: 181
196 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
197
198 IP: 192.168.137.227:43031 -> 31.13.68.16:443
199 Type: IP
200 Length: 104
201 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
202
203 IP: 31.13.82.36:443 -> 192.168.137.227:36280
204 Type: IP
205 Length: 341
206 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
207
208 IP: 192.168.137.227:36280 -> 31.13.82.36:443
209 Type: IP
210 Length: 337
211 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
212
213 IP: 31.13.82.36:443 -> 192.168.137.227:36287
214 Type: IP
215 Length: 381
216 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
217
218 IP: 192.168.137.227:36287 -> 31.13.82.36:443

219 Type: IP
220 Length: 389
221 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
222
223 IP: 31.13.82.36:443 -> 192.168.137.227:36290
224 Type: IP
225 Length: 301
226 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
227
228 IP: 192.168.137.227:36290 -> 31.13.82.36:443
229 Type: IP
230 Length: 285
231 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
232
233 IP: 31.13.68.16:443 -> 192.168.137.227:43040
234 Type: IP
235 Length: 181
236 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
237
238 IP: 31.13.82.1:443 -> 192.168.137.227:49699
239 Type: IP
240 Length: 301
241 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
242
243 IP: 192.168.137.227:43040 -> 31.13.68.16:443
244 Type: IP
245 Length: 104
246 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
247
248 IP: 192.168.137.227:49699 -> 31.13.82.1:443
249 Type: IP
250 Length: 285
251 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
252
253 IP: 192.168.137.227:52555 -> 192.168.137.1:53
254 Type: IP
255 Length: 71
256 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
257
258 IP: 192.168.137.227:35697 -> 192.168.137.1:53
259 Type: IP
260 Length: 71
261 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
262
263 IP: 192.168.137.1:53 -> 192.168.137.227:52555
264 Type: IP
265 Length: 87
266 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
267
268 IP: 192.168.137.1:53 -> 192.168.137.227:35697
269 Type: IP
270 Length: 87
271 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
272
273 IP: 192.168.137.1:49362 -> 239.255.255.250:1900

```
274 Type: IP
275 Length: 804
276 MAC: 22:53:49:24:ae:9a -> 01:00:5e:7f:ff:fa
277
278 IP: 172.217.24.142:443 -> 192.168.137.227:44905
279 Type: IP
280 Length: 52
281 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
282
283 IP: 192.168.137.227:44905 -> 172.217.24.142:443
284 Type: IP
285 Length: 52
286 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
287
288 IP: 192.168.137.227:58264 -> 192.168.137.1:53
289 Type: IP
290 Length: 75
291 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
292
293 IP: 192.168.137.1:53 -> 192.168.137.227:58264
294 Type: IP
295 Length: 142
296 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
297
298 IP: 203.119.218.243:80 -> 192.168.137.227:51510
299 Type: IP
300 Length: 120
301 MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96
302
303 IP: 192.168.137.227:51510 -> 203.119.218.243:80
304 Type: IP
305 Length: 120
306 MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a
307
308 IP: 192.168.137.1:55547 -> 239.255.255.250:1900
309 Type: IP
310 Length: 804
311 MAC: 22:53:49:24:ae:9a -> 01:00:5e:7f:ff:fa
```

共找到 62 个组流，除 1 个 IPv6 格式报文外，其余全部为 IP 格式的报文。

实验总结

通过本次实验，加深了对网络协议格式的理解，掌握了组流的基本概念，学会了 PCAP 的解百纳处理方法及 dpkt 的基本使用。为网络测量的实践打下基础。