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：

```python
f = open('test0.pcap', "rb")
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。

```python
flow_len = {}

for timestamp, buf in pcap:

    eth = dpkt.ethernet.Ethernet(buf)
    ip = eth.data

    fingerprint = str(str(ip.data.sport) + "," + str(ip.data.dport) + "," + str(
        eth.type) + "," + inet_to_str(ip.src) + "," + inet_to_str(ip.dst))
    if fingerprint in flow_len:
        flow_len[fingerprint][2] += len(ip)
    else:
        flow_len[fingerprint] = [mac_addr(eth.src), mac_addr(eth.dst) , 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：

```python
print("Number of flows: " + str(len(flow_len)) + "\n")

for key, value in flow_len.items():
    key_list = key.split(",")
    print("IP: " + key_list[3] + ":" + key_list[0] + " -> " + key_list[4] + ":" + key_list[1])

    if key_list[2] == str(dpkt.ethernet.ETH_TYPE_IP):
        print("Type: IP")
    elif key_list[2] == str(dpkt.ethernet.ETH_TYPE_IP6):
        print("Type: IPv6")

    print("Length: " + str(value[2]))
    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：

```
Number of flows: 6

IP: 192.168.137.227:36291 -> 31.13.82.36:443
Type: IP
Length: 41251
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36291
Type: IP
Length: 1418273
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36388 -> 31.13.68.16:443
Type: IP
Length: 5712
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43030
Type: IP
Length: 988981
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43030 -> 31.13.68.16:443
Type: IP
Length: 38802
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:36388
Type: IP
Length: 99120
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：

```
Number of flows: 62

IP: 192.168.137.227:36291 -> 31.13.82.36:443
Type: IP
Length: 41251
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36291
Type: IP
Length: 1418273
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36388 -> 31.13.68.16:443
Type: IP
Length: 5712
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43030
Type: IP
Length: 988981
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43030 -> 31.13.68.16:443
Type: IP
Length: 38802
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:36388
Type: IP
Length: 99120
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:49685 -> 31.13.82.1:443
Type: IP
Length: 28167
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:43039 -> 31.13.68.16:443
Type: IP
Length: 4033
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.1:443 -> 192.168.137.227:49685
Type: IP
Length: 76378
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 31.13.68.16:443 -> 192.168.137.227:43039
Type: IP
Length: 85675
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43029 -> 31.13.68.16:443
```

```
Type: IP
Length: 1430
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.34:443 -> 192.168.137.227:53351
Type: IP
Length: 3938
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:53351 -> 31.13.82.34:443
Type: IP
Length: 7246
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43029
Type: IP
Length: 8012
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:63282 -> 192.168.137.1:53
Type: IP
Length: 71
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:63282
Type: IP
Length: 87
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:50262 -> 31.13.68.13:443
Type: IP
Length: 239749
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:40723 -> 31.13.68.13:443
Type: IP
Length: 190641
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.13:443 -> 192.168.137.227:50262
Type: IP
Length: 6860167
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 31.13.68.13:443 -> 192.168.137.227:40723
Type: IP
Length: 4173536
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:5353 -> 224.0.0.251:5353
Type: IP
Length: 1260
MAC: fc:db:b3:e9:37:96 -> 01:00:5e:00:00:fb

IP: 192.168.137.227:48194 -> 192.168.137.1:53
```

```
Type: IP
Length: 67
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:48194
Type: IP
Length: 106
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43042 -> 31.13.68.16:443
Type: IP
Length: 42571
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43042
Type: IP
Length: 1551478
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43034 -> 31.13.68.16:443
Type: IP
Length: 3803
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43034
Type: IP
Length: 99268
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:42355 -> 192.168.137.1:53
Type: IP
Length: 75
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:42355
Type: IP
Length: 142
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:61764 -> 192.168.137.1:53
Type: IP
Length: 86
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:61764
Type: IP
Length: 86
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: fe80::6887:ef8:5ff2:e052:546 -> ff02::1:2:547
Type: IPv6
Length: 143
MAC: 22:53:49:24:ae:9a -> 33:33:00:01:00:02

IP: 192.168.137.227:36857 -> 121.51.131.223:8081
```

```
Type: IP
Length: 1317
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 121.51.131.223:8081 -> 192.168.137.227:36857
Type: IP
Length: 412
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 31.13.82.1:443 -> 192.168.137.227:49686
Type: IP
Length: 221
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:49686 -> 31.13.82.1:443
Type: IP
Length: 239
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36282
Type: IP
Length: 181
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36282 -> 31.13.82.36:443
Type: IP
Length: 104
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43031
Type: IP
Length: 181
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43031 -> 31.13.68.16:443
Type: IP
Length: 104
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36280
Type: IP
Length: 341
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36280 -> 31.13.82.36:443
Type: IP
Length: 337
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36287
Type: IP
Length: 381
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36287 -> 31.13.82.36:443
```

```
Type: IP
Length: 389
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.82.36:443 -> 192.168.137.227:36290
Type: IP
Length: 301
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:36290 -> 31.13.82.36:443
Type: IP
Length: 285
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 31.13.68.16:443 -> 192.168.137.227:43040
Type: IP
Length: 181
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 31.13.82.1:443 -> 192.168.137.227:49699
Type: IP
Length: 301
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:43040 -> 31.13.68.16:443
Type: IP
Length: 104
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:49699 -> 31.13.82.1:443
Type: IP
Length: 285
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:52555 -> 192.168.137.1:53
Type: IP
Length: 71
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:35697 -> 192.168.137.1:53
Type: IP
Length: 71
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:52555
Type: IP
Length: 87
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.1:53 -> 192.168.137.227:35697
Type: IP
Length: 87
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.1:49362 -> 239.255.255.250:1900
```

```
Type: IP
Length: 804
MAC: 22:53:49:24:ae:9a -> 01:00:5e:7f:ff:fa

IP: 172.217.24.142:443 -> 192.168.137.227:44905
Type: IP
Length: 52
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:44905 -> 172.217.24.142:443
Type: IP
Length: 52
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.227:58264 -> 192.168.137.1:53
Type: IP
Length: 75
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:53 -> 192.168.137.227:58264
Type: IP
Length: 142
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 203.119.218.243:80 -> 192.168.137.227:51510
Type: IP
Length: 120
MAC: 22:53:49:24:ae:9a -> fc:db:b3:e9:37:96

IP: 192.168.137.227:51510 -> 203.119.218.243:80
Type: IP
Length: 120
MAC: fc:db:b3:e9:37:96 -> 22:53:49:24:ae:9a

IP: 192.168.137.1:55547 -> 239.255.255.250:1900
Type: IP
Length: 804
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。