厦門大學

信息学院软件工程系

《计算机网络》实验报告

题　　目 实验三　用 PCAP 库监听并分析以太网的帧

班　　级 软件工程 2018 级 1 班

姓　　名 潘登

学　　号 24320182203249

实验时间 2020 年 3 月 11 日

2020 年　3 月 11　日

1 实验目的

用 PCAP 库编写程序实现对以太网的帧的监听，并按照要求输出监听的信息

2 实验环境

Win10　Visual Studio 2019　　C 语言

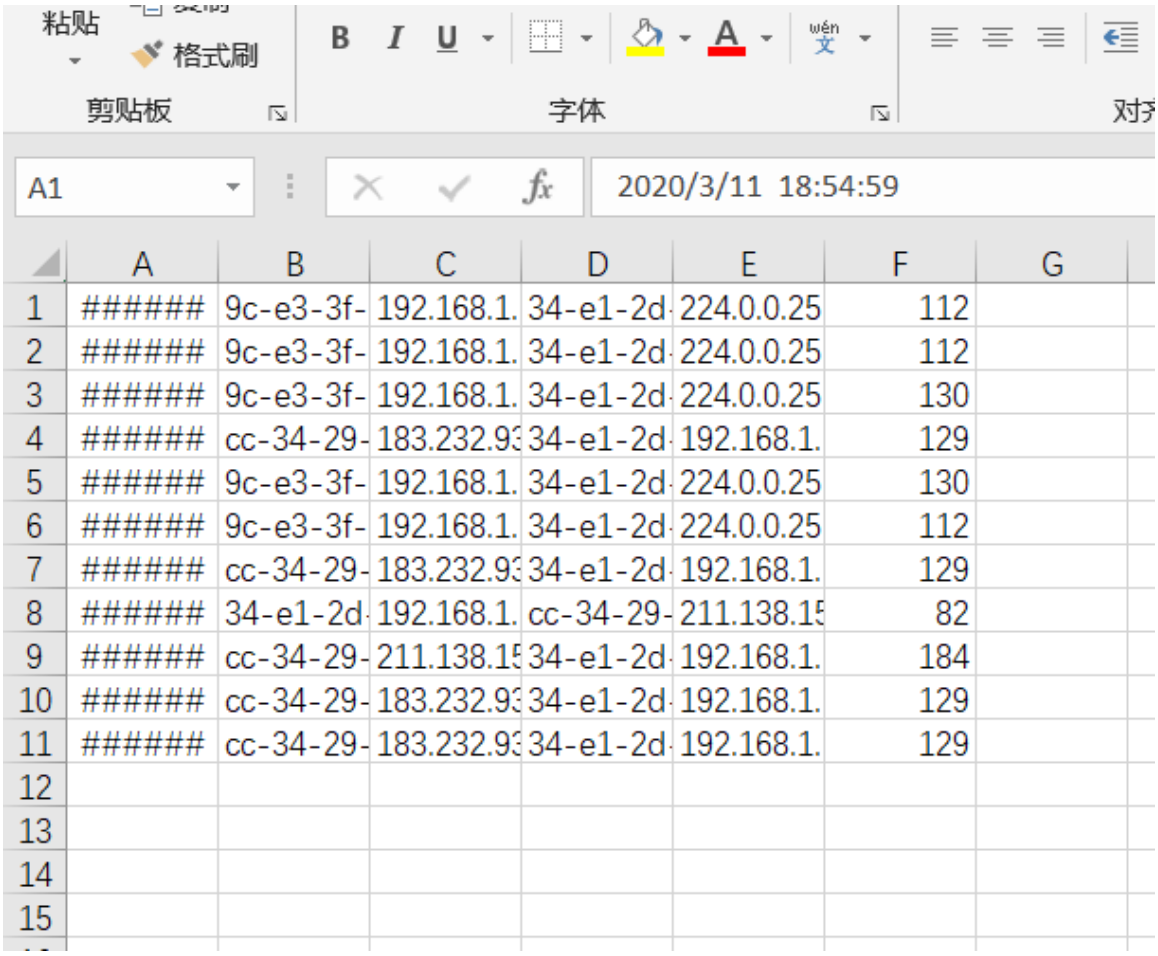
3 实验结果

```
2020-03-11 18:52:36 ,34-e1-2d-cf-1e-fd,192.168.26.6,7c-cc-1f-2e-3c-d0,218.85.157.99,68
2020-03-11 18:52:36 ,7c-cc-1f-2e-3c-d0,218.85.157.99,34-e1-2d-cf-1e-fd,192.168.26.6,157
```

1	0.000000	192.168.26.6	218.85.157.99	DNS	68 Standard query 0x2251 AAAA w.url.cn
2	0.000010	192.168.26.6	218.85.157.99	DNS	68 Standard query 0x2251 AAAA w.url.cn
3	0.021028	218.85.157.99	192.168.26.6	DNS	157 Standard query response 0x2251 AAAA w.url.cn CNAME newcomm.weixin.qq.com SOA ns-tel1.qq.com
4	0.021038	218.85.157.99	192.168.26.6	DNS	157 Standard query response 0x2251 AAAA w.url.cn CNAME newcomm.weixin.qq.com SOA ns-tel1.qq.com

在网卡 all-denied 状态下尝试用科莱数据包播放器播放之前用 wireshark 获得的数据包，得到正确结果

```
listening on Microsoft...
2020-03-11 18:54:59 ,9c-e3-3f-94-31-a7,192.168.1.105,34-e1-2d-cf-1e-fd,224.0.0.251,112
2020-03-11 18:55:00 ,9c-e3-3f-94-31-a7,192.168.1.105,34-e1-2d-cf-1e-fd,224.0.0.251,112
2020-03-11 18:55:02 ,9c-e3-3f-94-31-a7,192.168.1.105,34-e1-2d-cf-1e-fd,224.0.0.251,130
2020-03-11 18:55:02 ,cc-34-29-20-31-6a,183.232.93.22,34-e1-2d-cf-1e-fd,192.168.1.116,129
2020-03-11 18:55:03 ,9c-e3-3f-94-31-a7,192.168.1.105,34-e1-2d-cf-1e-fd,224.0.0.251,130
2020-03-11 18:55:03 ,9c-e3-3f-94-31-a7,192.168.1.105,34-e1-2d-cf-1e-fd,224.0.0.251,112
2020-03-11 18:55:04 ,cc-34-29-20-31-6a,183.232.93.22,34-e1-2d-cf-1e-fd,192.168.1.116,129
2020-03-11 18:55:09 ,34-e1-2d-cf-1e-fd,192.168.1.116,cc-34-29-20-31-6a,211.138.151.161,82
2020-03-11 18:55:09 ,cc-34-29-20-31-6a,211.138.151.161,34-e1-2d-cf-1e-fd,192.168.1.116,184
2020-03-11 18:55:11 ,cc-34-29-20-31-6a,183.232.93.22,34-e1-2d-cf-1e-fd,192.168.1.116,129
2020-03-11 18:55:15 ,cc-34-29-20-31-6a,183.232.93.22,34-e1-2d-cf-1e-fd,192.168.1.116,129
```

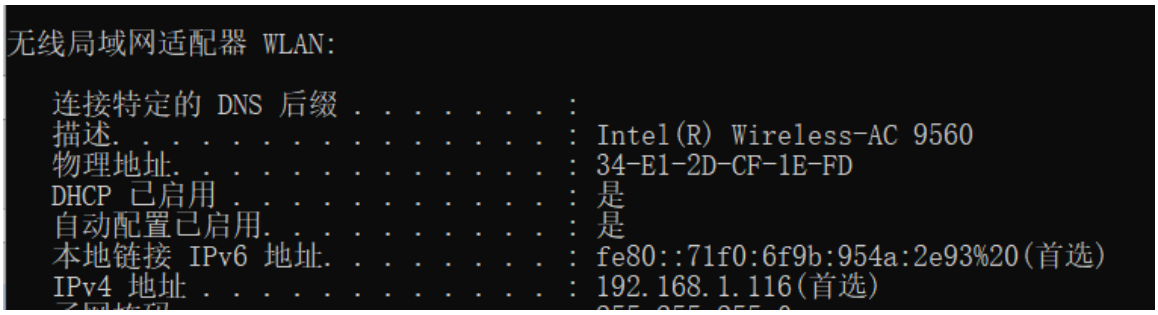


粘贴 格式刷 剪贴板 字体 对齐

A1 2020/3/11 18:54:59

	A	B	C	D	E	F	G
1	######	9c-e3-3f-	192.168.1.	34-e1-2d	224.0.0.25	112	
2	######	9c-e3-3f-	192.168.1.	34-e1-2d	224.0.0.25	112	
3	######	9c-e3-3f-	192.168.1.	34-e1-2d	224.0.0.25	130	
4	######	cc-34-29-	183.232.93	34-e1-2d	192.168.1.	129	
5	######	9c-e3-3f-	192.168.1.	34-e1-2d	224.0.0.25	130	
6	######	9c-e3-3f-	192.168.1.	34-e1-2d	224.0.0.25	112	
7	######	cc-34-29-	183.232.93	34-e1-2d	192.168.1.	129	
8	######	34-e1-2d	192.168.1.	cc-34-29-	211.138.15	82	
9	######	cc-34-29-	211.138.15	34-e1-2d	192.168.1.	184	
10	######	cc-34-29-	183.232.93	34-e1-2d	192.168.1.	129	
11	######	cc-34-29-	183.232.93	34-e1-2d	192.168.1.	129	
12							
13							
14							
15							

在网络（WLAN）正常开启状态下监听，并将结果输出到对应的 csv 文件里，数据完全一致



```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Intel(R) Wireless-AC 9560
   物理地址. . . . . : 34-E1-2D-CF-1E-FD
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::71f0:6f9b:954a:2e93%20(首选)
   IPv4 地址 . . . . . : 192.168.1.116(首选)
```

在命令行窗口查看无限局域网 MAC 地址和 IP，与上述结果对照检查，结果正确

4 实验总结

本次实验让我对以太网的帧有了更深刻的了解，包括如用软件何监听以太网的帧，分析得到的帧，帧的格式，以及使用 Winpcap 库编写程序对以太网的帧进行监听，加深了我对计算机网络数据链路层的理解。

本次实验还让我修改第三方代码的能力得到提升，也增加了我对 C 语言的熟练度