课程名 计算机网络

实验名称:	实验 3
实验日期:	2021 年.4 月 2 日

学号:	22920192204245
姓名:	刘冰帅
专业年级:	大二
学年学期:	2020-2021 春季

基于 PCAP 库侦听并分析网络流量

1. 实验目的

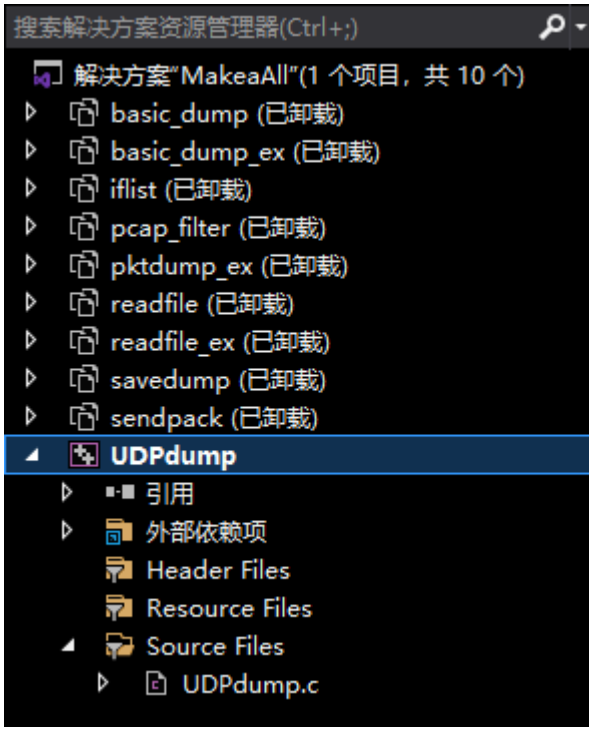
通过完成实验，理解数据链路层、网络层、传输层和应用层的基本原理。掌握用 Wireshark 观察网络流量并辅助网络侦听相关的编程；掌握用 Libpcap 或 WinPcap 库侦听并处理以太网帧和 IP 报文的方法；熟悉以太网帧、IP 报文、TCP 段和 FTP 命令的格式概念，掌握 TCP 协议的基本机制；熟悉帧头部或 IP 报文头部各字段的含义。熟悉 TCP 段和 FTP 数据协议的概念，熟悉段头部各字段和 FTP 控制命令的指令和数据的含义。

2. 用户需求

2.1 用侦听解析软件观察数据格式
2.2 用侦听解析软件观察 TCP 机制
2.3 用 Libpcap 或 WinPcap 库侦听网络数据
2.4 解析侦听到的网络数据

3. 实验过程

1. 首先下载安装 WireShark 和科来数据包播放器。
2. 下载 Wpdpack 压缩文件，打开 MakeAll 项目，卸载除 UDPdump 以外的所有其他工项目。



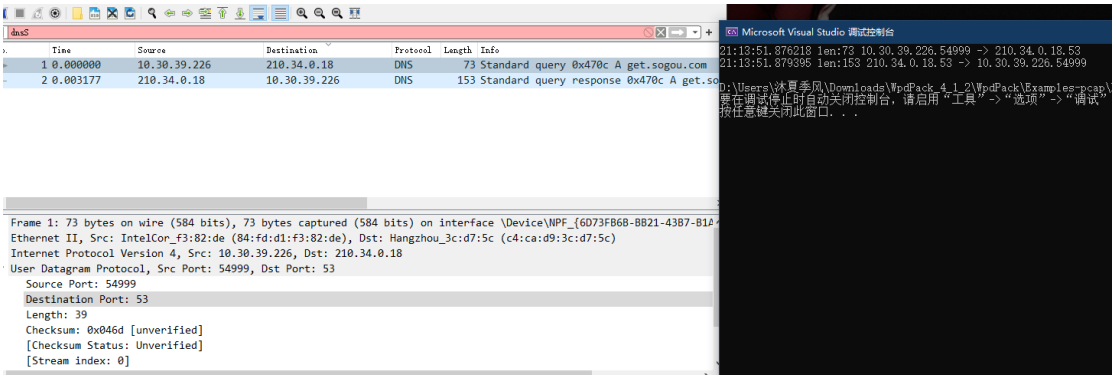
3. 打开 WireShark，限定搜索条件为 DNS，停止监听，选择前两项记录，另存为 dns.pcap

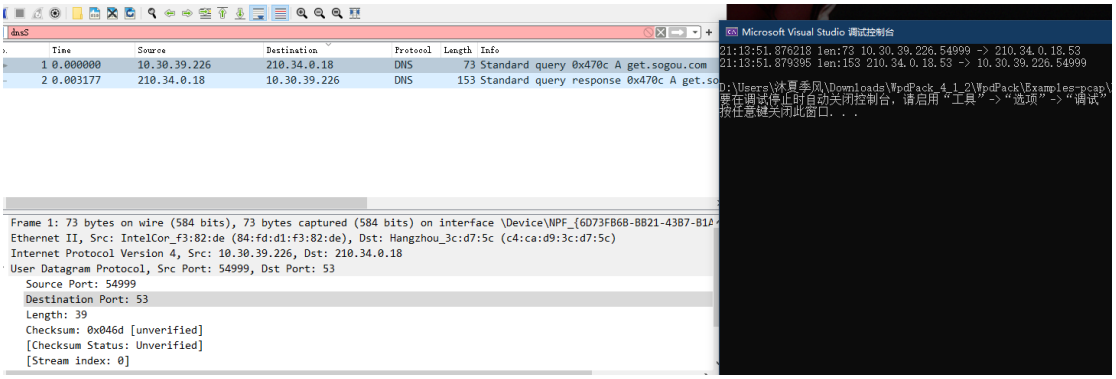
1	0.000000	10.30.39.226	210.34.0.18	DNS	73 Standard query 0x470c A get.sogou.com
2	0.003177	210.34.0.18	10.30.39.226	DNS	153 Standard query response 0x470c A get.sogou.com A 39.156.167.33 A 39.156.165.34 A 39.156.165.32 A 39.156.165.33 A 39.156.167.32

4. 从 readfile 项目中选择读取文件的代码片段，插入到 UDPdump.c 主函数中，为之后的操作做准备。

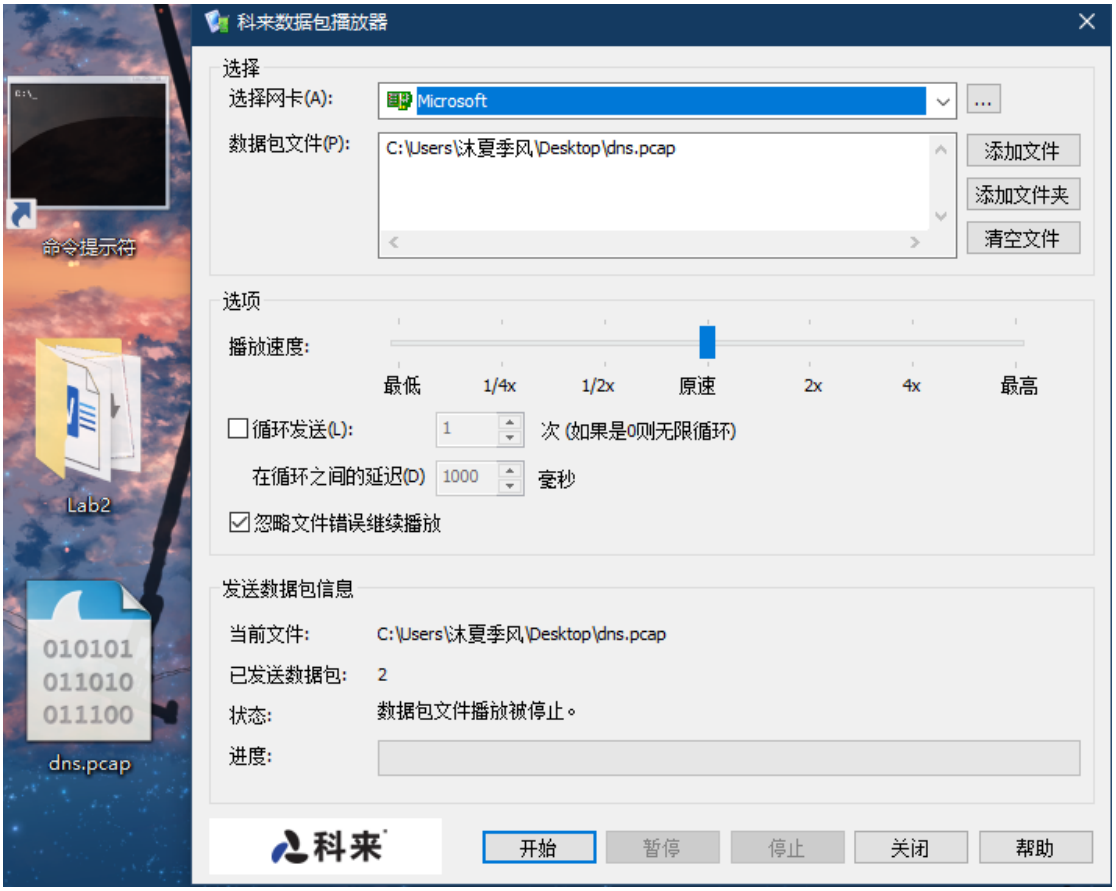
```
#define FROM_NIC
int main()
{
    pcap_if_t *alldevs;
    pcap_if_t *d;
    int inum;
    int i=0;
    pcap_t *adhandle;
    char errbuf[PCAP_ERRBUF_SIZE];
    u_int netmask;
    char packet_filter[] = "ip and udp";
    struct bpf_program fcode;
#ifdef FROM_NIC 活动预处理器块
#else
    if ((adhandle = pcap_open_offline("C:\\Users\\沐夏季风\\Desktop\\dns.pcap",
        errbuf          // error buffer
    )) == NULL)
    {
        fprintf(stderr, "\nUnable to open the file.\n");
        return -1;
    }
    /* read and dispatch packets until EOF is reached */
    pcap_loop(adhandle, 0, packet_handler, NULL);
    pcap_close(adhandle);
#endif
    return 0;
}
```

5. 注释掉#define FROM_NIC 语句，运行读取文件代码块，对比读取后的文件和 WireShark 中的信息，了解报文的构成。

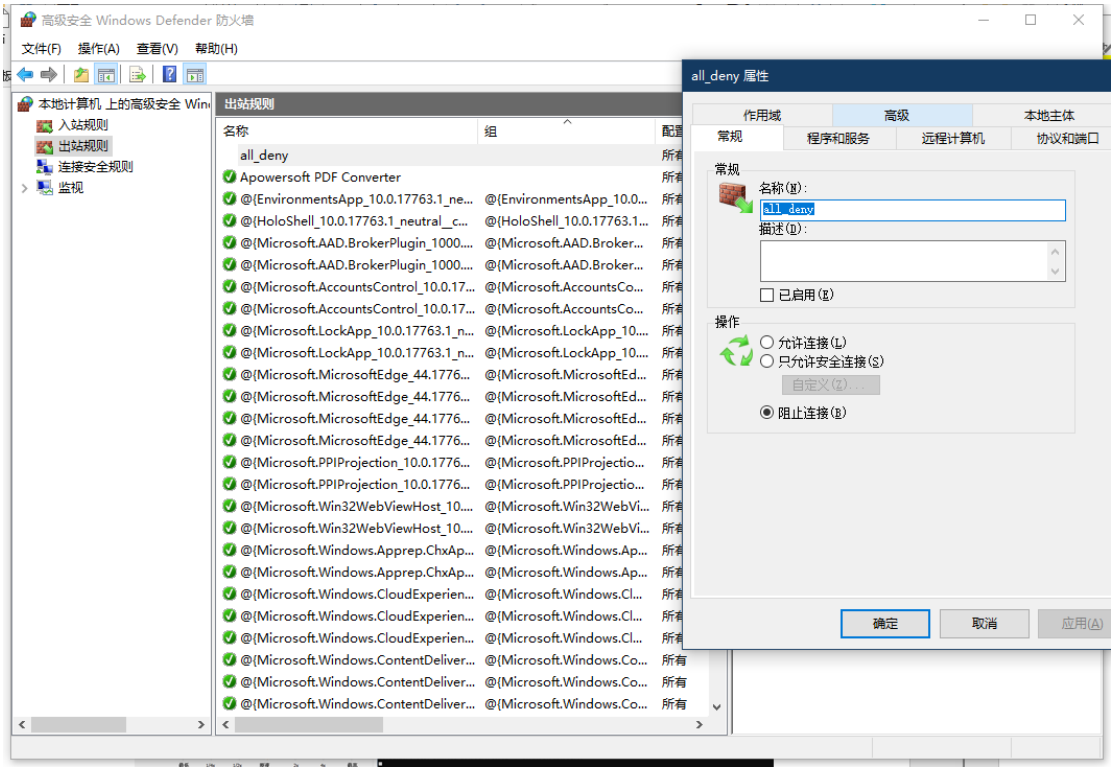




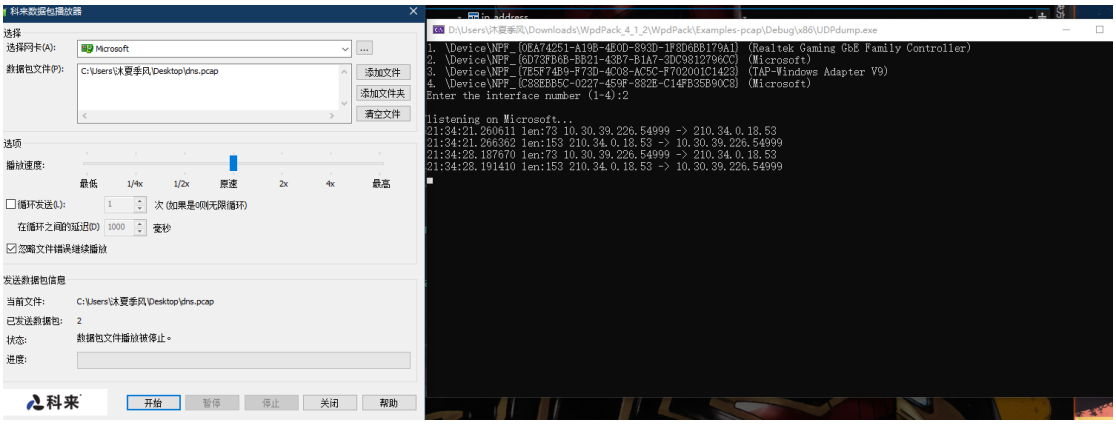
6. 打开科来数据包播放器，添加正确的网卡以及 dns.pcap 文件



7. 打开高级防火墙，新建出站规则 all_deny，阻塞网络，防止侦听到其他干扰项。



8. 取消注释#define FROM_NIC 语句，使程序正常侦听网络，选择正确的网卡（与之前科来数据包播放器相同）。
9. 此时可以观察到，由于之前阻塞网络的操作，此时无法侦听到任何数据，判断已经排除其他干扰项。
10. 使用科来数据包播放器的开始按钮，播放报文，观察程序侦听结果。



侦听结果与原报文完全相同。