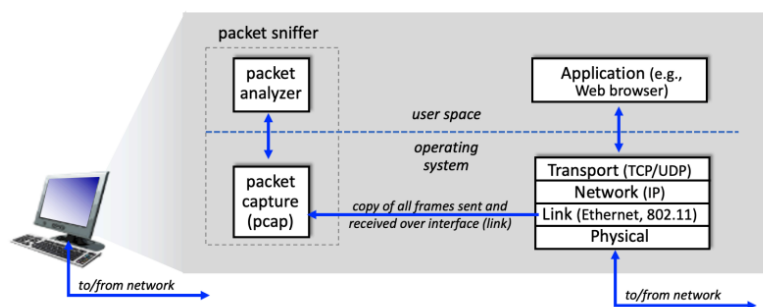


学号：202000130143	姓名： 郑凯饶	班级： 2020 级 1 班
实验题目：Wireshark introduction		
实验学时： 2	实验日期： 3. 1	
实验目的： 熟悉 Wireshark，尝试简单的网络抓包操作。		
硬件环境： Dell Latitude 5411 Intel (R) Core(TM) i5-10400H CPU @ 2. 60GHz (8GPUs) , ~2. 6GHz		
软件环境： Windows 10 家庭中文版 64 位（10. 0，版本 18363） Wireshark-win64-3. 6. 2		
实验步骤与内容： 1. 问题： 1) 列举几种不同的网络协议。 2) HTTP GET 和 OK 之间间隔了多久？ 3) 本机地址及 gaia. cs. umass. edu 地址。 4) 打印 HTTP 报文。 2. 阐述基本方法 下载 Wireshark 及 npcap。 使用 Wireshark 进行抓包分析。		



The diagram illustrates the packet sniffer structure. It shows a laptop connected to a network. Data flows from the network into the operating system (OS) layer, which contains the Link (Ethernet, 802.11) and Physical layers. A packet capture (pcap) component in the OS layer captures all frames sent and received over the interface. This data is then passed to the user space, where a packet analyzer processes the captured data. The user space also contains an application (e.g., Web browser) that interacts with the network through the Transport (TCP/UDP) and Network (IP) layers. The diagram shows the flow of data from the network, through the OS layers, to the user space application, and back to the network.

Figure 1: packet sniffer structure

由图可知，包嗅探分为抓包和包分析两部分，抓包是在数据链路层进行的，包分析将报文信息给用户。

3. 实验结果展示与分析

1) 列举几种不同的网络协议。
TCP, UDP, DNS, HTTP, DHCP, TLSv1. 2

2) HTTP GET 和 OK 之间间隔了多久？

Time	Source	Destination	Protocol	Length	Info
2022-03-06 21:00:38.402171	172.25.218.140	128.119.245.12	HTTP	545	GET /wireshark-labs/INTRO-wire
2022-03-06 21:00:38.667025	128.119.245.12	172.25.218.140	HTTP	436	HTTP/1.1 200 OK (text/html)
2022-03-06 21:00:38.695085	172.25.218.140	128.119.245.12	HTTP	491	GET /favicon.ico HTTP/1.1
2022-03-06 21:00:38.963743	128.119.245.12	172.25.218.140	HTTP	483	HTTP/1.1 404 Not Found (text/

3) 本机地址及 gaia.cs.umass.edu 地址。

172.25.218.140 为本机地址，128.119.245.12 为 gaia.cs.umass.edu 地址。

4) 打印 HTTP 报文。

```
No.      Time      Source      Destination      Protocol Length Info
 55 15.020572 172.25.243.108 128.119.245.12  HTTP      627  GET /wireshark-labs/INTRO-
wireshark-file1.html HTTP/1.1
Frame 55: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{5387F7EC-
BB57-4339-86BC-87E740046725}, id 0
Ethernet II, Src: e2:d1:01:36:15:f7 (e2:d1:01:36:15:f7), Dst: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)
Destination: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)
Source: e2:d1:01:36:15:f7 (e2:d1:01:36:15:f7)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.25.243.108, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50233, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
Hypertext Transfer Protocol
No.      Time      Source      Destination      Protocol Length Info
 57 15.312176 128.119.245.12 172.25.243.108  HTTP      237  HTTP/1.1 304 Not Modified
Frame 57: 237 bytes on wire (1896 bits), 237 bytes captured (1896 bits) on interface \Device\NPF_{5387F7EC-
BB57-4339-86BC-87E740046725}, id 0
Ethernet II, Src: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: e2:d1:01:36:15:f7 (e2:d1:01:36:15:f7)
Destination: e2:d1:01:36:15:f7 (e2:d1:01:36:15:f7)
Source: JuniperN_f6:12:a0 (28:a2:4b:f6:12:a0)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.25.243.108
Transmission Control Protocol, Src Port: 80, Dst Port: 50233, Seq: 1, Ack: 574, Len: 183
Hypertext Transfer Protocol
```

结论分析与体会：

配置 npcap 是勾选了管理员权限限制的选项，开启时不断碰到请求权限的询问。软件每检测到一个网络端口就会询问一次，可以直接使用管理员权限打开。期待用 Wireshark 进行更进一步的报文分析。