实验一 WireShark 的安装和运行

专业班级： 信息安全智息技术班 **学号：** 21307130076 **姓名：** 杨乙

【实验目的】

1.WireShark 的安装以及界面熟悉
2.简单 HTTP 的抓取和过滤，结果进行分析和导出

【实验步骤】

1.打开 Wireshark
2.选择“捕获”下拉菜单，选择“选项”，Input 选择 WLAN
3.点击“开始”，启动捕获
4.在浏览器中输入给定的 URL，在浏览器中显示该界面
5.显示界面后，在 Wireshark 中点击停止按钮来停止 Wireshark 分组捕获
6.在主 Wireshark 窗口顶部的分组显示过滤器窗口中键入 http 然后选择应用，以只将 HTTP 消息显示在分组列表窗口中
7.找到发送到 gaia.cs.umass.edu HTTP 服务器的 HTTP GET 消息。选择消息以查看协议相关的相关信息
8.打印 GET 和 OK 两个 HTTP 消息
9.退出 Wireshark

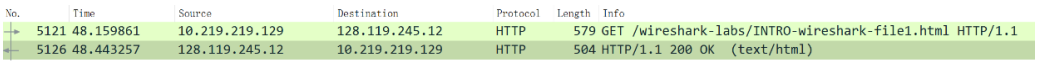
【实验结果】

分析操作，回答问题。

1.列出上述步骤 f 中出现在未过滤的分组列表窗口的协议列中的 3 种不同的协议。

TCP 协议 ARP 协议 DNS 协议

2.从 HTTP GET 消息发送到 HTTP OK 回复需要多长时间?



No.	Time	Source	Destination	Protocol	Length	Info
5121	48.159861	10.219.219.129	128.119.245.12	HTTP	579	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
5126	48.443257	128.119.245.12	10.219.219.129	HTTP	504	HTTP/1.1 200 OK (text/html)

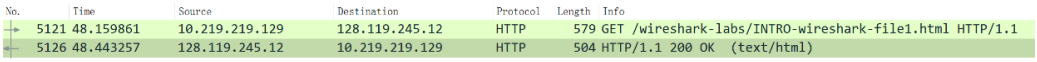
HTTP GET 消息发送距离开始捕获的时间：48.159861s

HTTP OK 回复距离开始捕获的时间：48.443257s

二者相距时间：48.443257s - 48.159861s = 0.283396s

3.gaia.cs.umass.edu(也称为 wwwnet.cs.umass.edu)的 Internet 地址是什么?

您的计算机的 Internet 地址是什么?



No.	Time	Source	Destination	Protocol	Length	Info
5121	48.159861	10.219.219.129	128.119.245.12	HTTP	579	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
5126	48.443257	128.119.245.12	10.219.219.129	HTTP	504	HTTP/1.1 200 OK (text/html)

客户端向 Web 服务器发送请求消息（本例中方法为 GET），在发送请求消息之后，Web 服务器会返回响应消息（本例中状态码为 200），因此，根据上图信息可以获得客户端（本计算机）和 Web 服务器的 Internet 地址：

gaia.cs.umass.edu：128.119.245.12

我的计算机的 Internet 地址：10.219.219.129

4.打印问题 2 提到的两个 HTTP 消息(GET 和 OK):

打印内容截图如下：

```
No.     Time           Source                Destination           Protocol Length Info
   5121 48.159861      10.219.219.129        128.119.245.12        HTTP     579    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 5121: 579 bytes on wire (4632 bits), 579 bytes captured (4632 bits) on interface \Device\NPF_{84F30BE1-7874-473F-
BB1D-9A7FAE3D946F}, id 0
Ethernet II, Src: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4), Dst: HuaweiTe_f2:be:11 (dc:99:14:f2:be:11)
Internet Protocol Version 4, Src: 10.219.219.129, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60662, Dst Port: 80, Seq: 1, Ack: 1, Len: 513
Hypertext Transfer Protocol

No.     Time           Source                Destination           Protocol Length Info
   5126 48.443257      128.119.245.12        10.219.219.129        HTTP     504    HTTP/1.1 200 OK  (text/html)
Frame 5126: 504 bytes on wire (4032 bits), 504 bytes captured (4032 bits) on interface \Device\NPF_{84F30BE1-7874-473F-
BB1D-9A7FAE3D946F}, id 0
Ethernet II, Src: HuaweiTe_f2:be:11 (dc:99:14:f2:be:11), Dst: IntelCor_0e:b9:c4 (98:8d:46:0e:b9:c4)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.219.219.129
Transmission Control Protocol, Src Port: 80, Dst Port: 60662, Seq: 1, Ack: 514, Len: 438
Hypertext Transfer Protocol
Line-based text data: text/html (3 lines)
    <html>\n
    Congratulations!  You've downloaded the first Wireshark lab file!\n
    </html>\n
```