计算机学院_计算机网络_课程实验报告

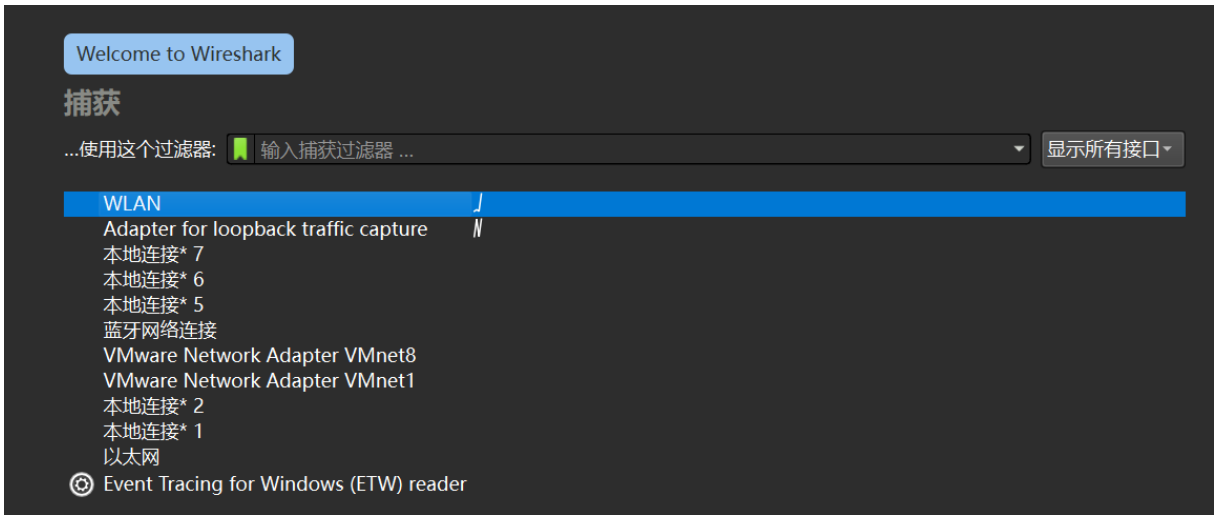
实验题目： 初步了解 WireShark1，并进行一些简单的数据包捕获和观察。		**学号：** 202200400053
日期： 2024-03-08	**班级：** 2 班	**姓名：** 王宇涵
Email：1941497679@qq.com		

实验方法介绍：

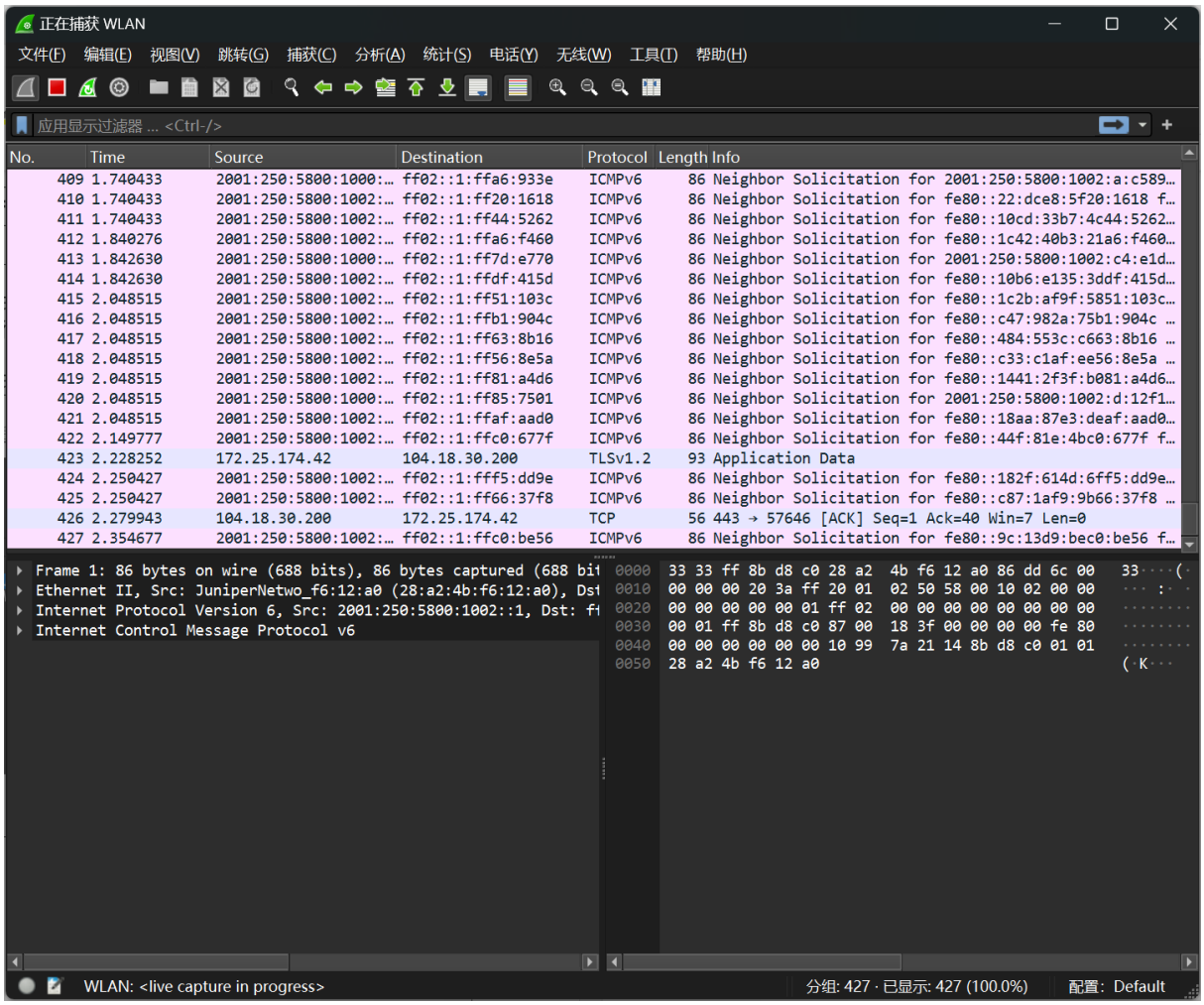
1. 了解 WireShark 抓包的原理
2. 通过下载，安装，初步运行 WireShark，了解界面的功能，进行简单的抓包过程，来理解数据的含义
3. 通过对数据含义的分析和理解加深对理论课学习的理解

实验过程描述：

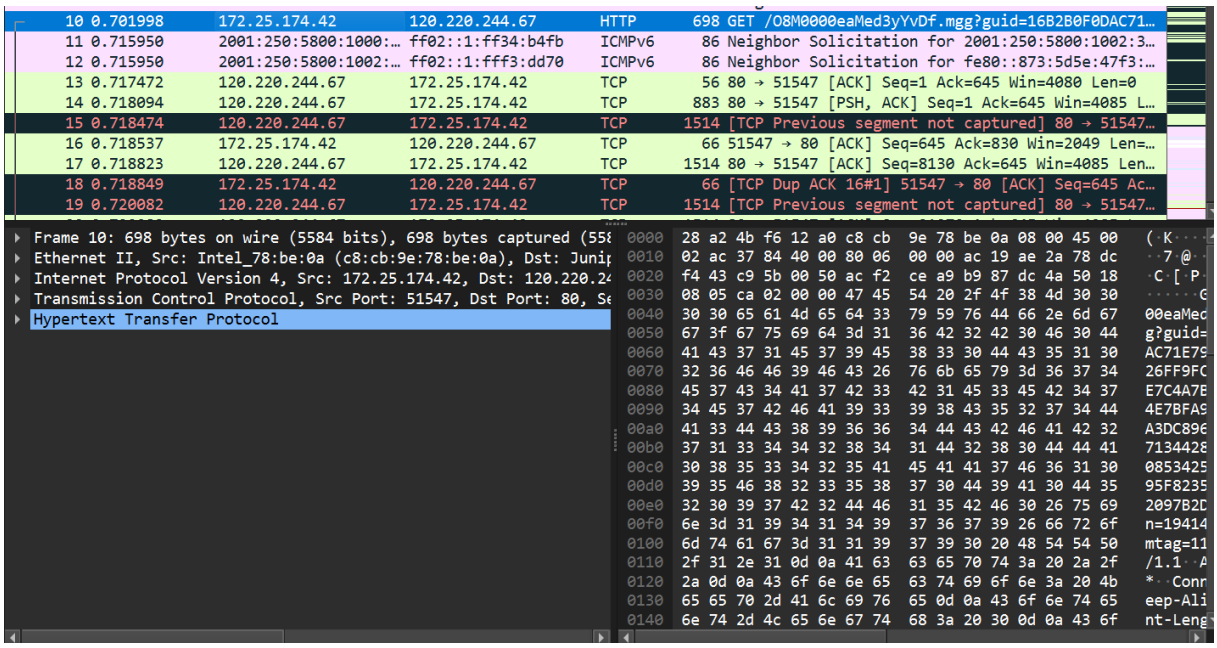
1. 启动 WireShark，选择合适的接口，我们这里选择 WLAN



2. 进入抓包页面



3. 分析界面 ：数据列从左到右依此是抓取的数据包编号，时间，发送源，到达地，协议类型，长度，详细信息
4. 单击某一条数据包，即可查到详细的数据包信息，包括有关以太网帧(假设数据包是通过以太网接口发送/接收的)和包含该数据包的 IP 数据报的信息

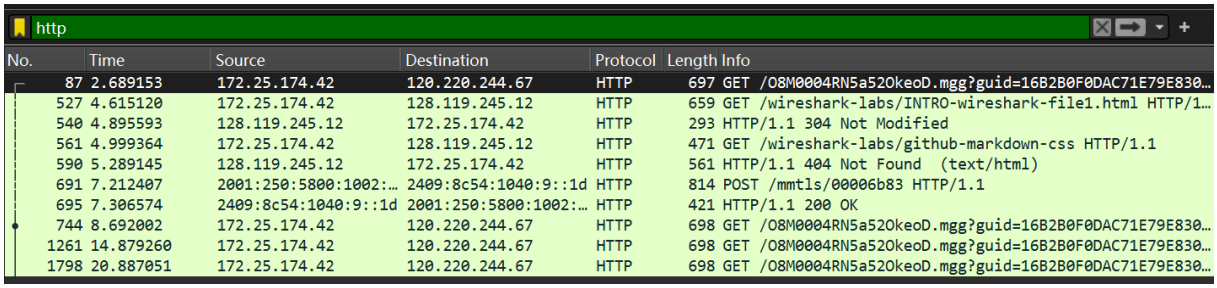


可以看出：数据包内容窗口以 ASCII 和十六进制格式显示捕获帧的全部内容

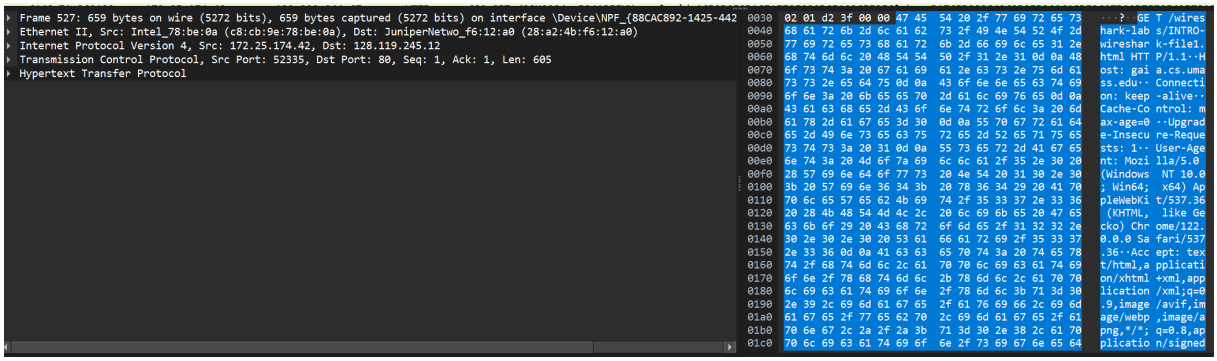
5. 进行测试：打开 WireShark 的捕获功能，打开浏览器输入网址 http://gaia.cs.umass.edu/Wireshark-labs/intro-Wireshark-file1.html，显示内容

Congratulations! You've downloaded the first Wireshark lab file!

回到 WireShark，在过滤行输入"http"：就可以查到网址的数据包



6. 点击 HTTP GET 数据包，查看详细信息



7. 回答实验有关问题(见结论分析)

结论分析：

1. 跟踪文件中显示了下列哪个协议(例如，在 Wireshark“协议”列中列出)：TCP、QUIC、HTTP、DNS、UDP、 TLSv1.2？

答 ：http 协议

2.从发送 HTTPGET 消息到收到 HTTPOK 应答需要多长时间？(默认情况下，信息包列表窗口中 Time 列的值是自 Wireshark 跟踪开始以来的时间量(以秒为单位)。(如果要以时间格式显示 Time 字段，请选择 WiresharkView 下拉菜单，然后选择 Time Display Format，再选择 Time-of-day。)

6634	67.224447	172.25.174.42	128.119.245.12	HTTP	548 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
6647	67.570824	128.119.245.12	172.25.174.42	HTTP	492 HTTP/1.1 200 OK (text/html)

答 ： 时间为 0.346377s

3.Gaia.cs.umass.edu 的互联网地址(亦称为 wwwnet)。Cs.umass.edu) ？您的计算机的 Internet 地址是什么，或者(如果您正在使用跟踪文件)发送 HTTPGET 消息的计算机的 Internet 地址是什么？

答 ：172.25.174.42

4.在 Wireshark“选定包的详细信息”窗口中展开 HTTP 消息上的信息(参见上面的图 3) ，这样您就可以看到 HTTP GET 请求消息中的字段。什么类型的 Web 浏览器发出了 HTTP 请求？答案显示在扩展的 HTTP 消息显示中“ User-Agent:”字段后面的信息的右端。[HTTP 消息中的这个字段值表示 Web 服务器如何了解您正在使用的浏览器类型。]Firefox，Safari，Microsoft Internet Edge，Other

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36\r\n
```

答 ：Safari

5.在 Wireshark 的“所选数据包的详细信息”窗口中展开该数据包的传输控制协议信息(参见实验室文档中的图 3) ，这样您就可以看到 TCP 段中携带 HTTP 消息的字段。这个 HTTP 请求被发送到的目的端口号是多少(在包含 HTTP 请求的 TCP 段的“ Dest Port:”之后的数字) ？

```
Transmission Control Protocol, Src Port: 53256, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
    Source Port: 53256
    Destination Port: 80
```

答 ：80

6.打印问题 2 中提到的两条 HTTP 消息(GET 和 OK)。要这样做，从 WiresharkFile 命令菜单中选择 Print，然后选择“ Selected Packet Only”和“ Print as display”径向按钮，然后单击 OK

答 ： 如 图

```
No.     Time           Source                Destination           Protocol Length Info
   6634 67.224447      172.25.174.42         128.119.245.12        HTTP     548    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 6634: 548 bytes on wire (4384 bits), 548 bytes captured (4384 bits) on interface
\Device\NPF_{88CAC892-1425-442F-84AB-F18E52D8913E}, id 0
Ethernet II, Src: Intel_78:be:0a (c8:cb:9e:78:be:0a), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
Internet Protocol Version 4, Src: 172.25.174.42, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 534
    Identification: 0x0bb7 (2999)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.25.174.42
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 53256, Dst Port: 80, Seq: 1, Ack: 1, Len: 494
    Source Port: 53256
    Destination Port: 80
    [Stream index: 54]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 494]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 4015310469
    [Next Sequence Number: 495    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 833400318
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 256
    [Calculated window size: 65536]
    [Window size scaling factor: 256]
    Checksum: 0xd1d0 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (494 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/
537.36\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/2]
    [Response in frame: 6647]
    [Next request in frame: 6654]
```

```
No.     Time           Source                Destination           Protocol Length Info
   6647 67.570824      128.119.245.12        172.25.174.42         HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 6647: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface
\Device\NPF_{88CAC892-1425-442F-84AB-F18E52D8913E}, id 0
Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: Intel_78:be:0a (c8:cb:9e:78:be:0a)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.25.174.42
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x74 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 478
    Identification: 0x0b6e (2926)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 43
    Protocol: TCP (6)
    Header Checksum: 0x7270 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 172.25.174.42
Transmission Control Protocol, Src Port: 80, Dst Port: 53256, Seq: 1, Ack: 495, Len: 438
    Source Port: 80
    Destination Port: 53256
    [Stream index: 54]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 833400318
    [Next Sequence Number: 439    (relative sequence number)]
    Acknowledgment Number: 495    (relative ack number)
    Acknowledgment number (raw): 4015310963
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xc578 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (438 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 200 OK\r\n
    Date: Sat, 09 Mar 2024 08:59:31 GMT\r\n
    Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3\r\n
    Last-Modified: Sat, 09 Mar 2024 06:59:02 GMT\r\n
    ETag: "51-61334d7edbe79"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 81\r\n
    Keep-Alive: timeout=5, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/2]
    [Time since request: 0.346377000 seconds]
    [Request in frame: 6634]
    [Next request in frame: 6654]
    [Next response in frame: 6744]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
Line-based text data: text/html (3 lines)
```

结论：

本次实验是对 WireShark 软件的初步认识，通过一个简单的抓包测试，分析 Get 和 Ok 数据包，加深了对于数据包，协议，端口等知识点的理解，也巩固了理论课的知识，让我收获良多.