# 计算机学院 计算机网络 课程实验报告

| | | |
|---|---|---|
| 实验题目： wireshark_intro | | 学号：202200130048 |
| 日期：2024.3.5 | 班级： 6 | 姓名： 陈静雯 |
| Email：1205037094@qq.com | | |

**实验方法介绍：**

输入网址观察抓包信息

**实验过程描述：**

1. 下载并安装 wireshark
2. 选择 WLAN 进行包捕获
3. 在 Wireshark 运行过程中，输入 URL：http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html
4. 当浏览器显示“INTRO-wireshark-file1.html”页面(只是一行简单的祝贺)后，在 Wireshark 抓包窗口中选择“stop”，停止 Wireshark 抓包。
5. 查看各种捕获的信息

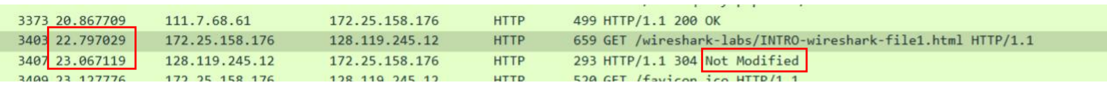
**结论分析：**

1. Which of the following protocols are shown as appearing (i.e., are listed in the Wireshark “protocol” column) in your trace file? 用到了哪些协议

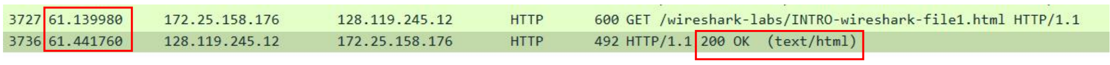
TCP，TLSv1.2，SSDP，ICMPv6，DNS，TLSv1.3，QUIC，ARP，UDP，MDNS，HTTP

2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? 花了多少时间

0.3s 有的时候刷新一下是 OK，但是大部分是 not modified，不知道为什么



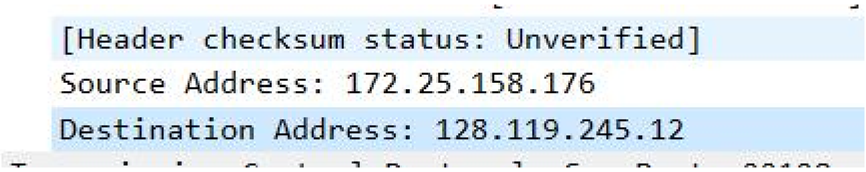
```
3373 20.867709   111.7.68.61      172.25.158.176   HTTP   499 HTTP/1.1 200 OK
3403 22.797029   172.25.158.176   128.119.245.12   HTTP   659 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3407 23.067119   128.119.245.12   172.25.158.176   HTTP   293 HTTP/1.1 304 Not Modified
3409 23.127776   172.25.158.176   128.119.245.12   HTTP   520 GET /favicon.ico HTTP/1.1
```



```
3727 61.139980   172.25.158.176   128.119.245.12   HTTP   600 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
3736 61.441760   128.119.245.12   172.25.158.176   HTTP   492 HTTP/1.1 200 OK  (text/html)
```

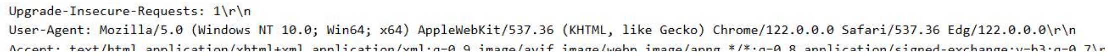
3. gaia.cs.umass.edu 的互联网地址 128.119.245.12

发送 HTTP GET 消息的计算机的 Internet：172.25.158.176



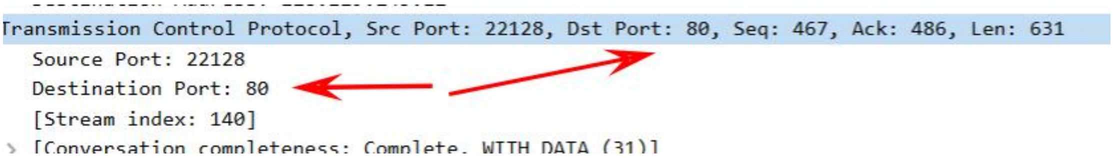
```
[Header checksum status: Unverified]
Source Address: 172.25.158.176
Destination Address: 128.119.245.12
```

4.web 浏览器类型，edg（Microsoft Internet Edge），chrome



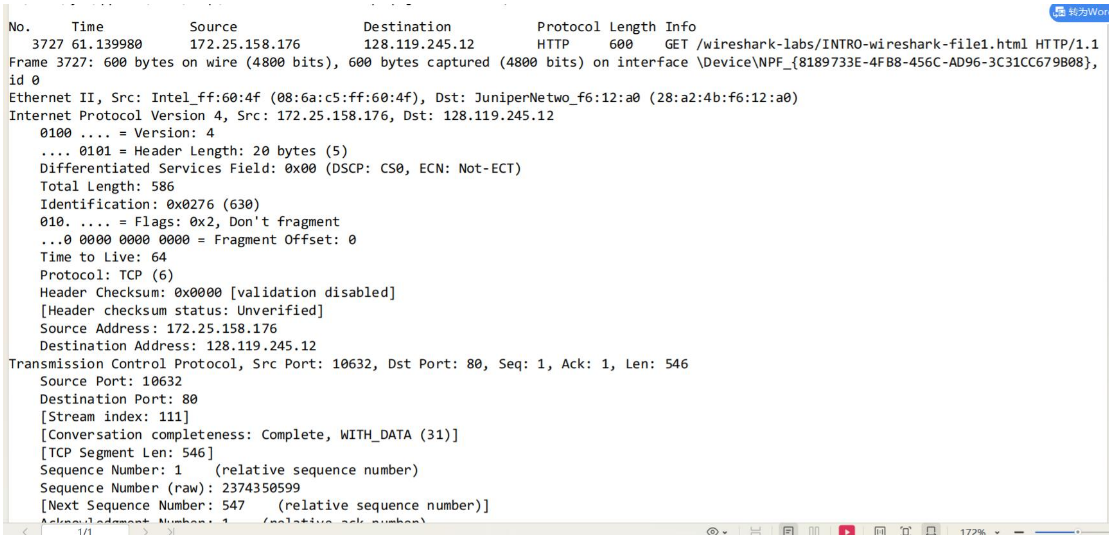
```
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r
```

5.包含 http 的 tcp 段：80

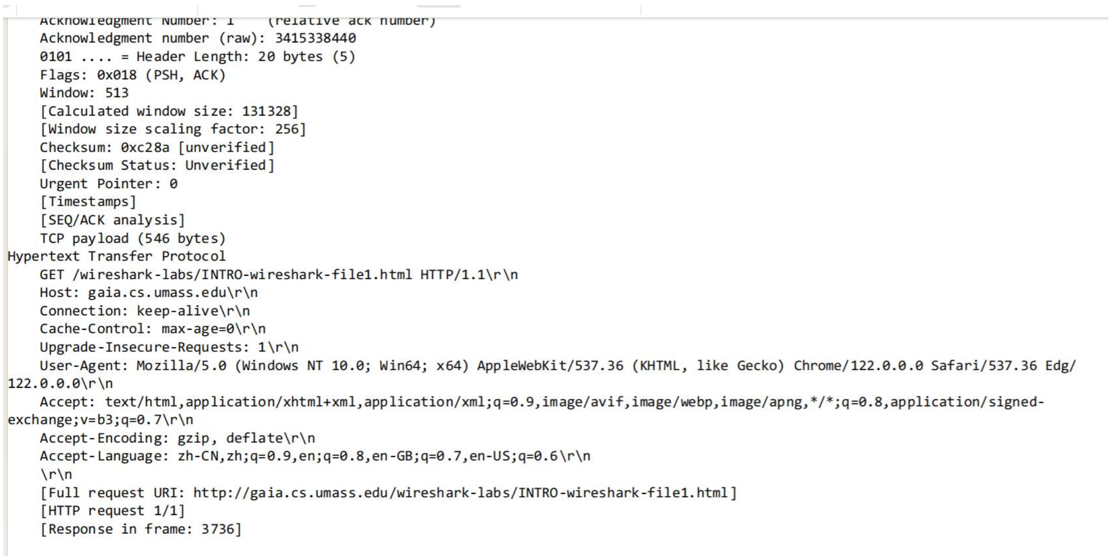


```
Transmission Control Protocol, Src Port: 22128, Dst Port: 80, Seq: 467, Ack: 486, Len: 631
    Source Port: 22128
    Destination Port: 80
    [Stream index: 140]
  > [Conversation completeness: Complete, WITH_DATA (31)]
```

6. 打印 get

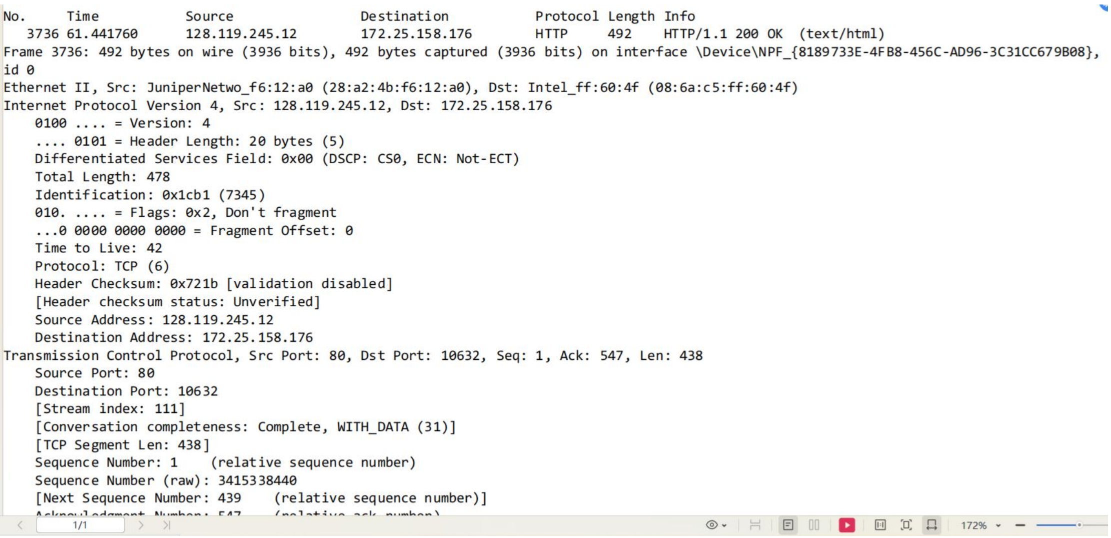


```
No.     Time           Source                Destination           Protocol Length Info
   3727 61.139980      172.25.158.176        128.119.245.12        HTTP     600    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 3727: 600 bytes on wire (4800 bits), 600 bytes captured (4800 bits) on interface \Device\NPF_{8189733E-4FB8-456C-AD96-3C31CC679B08},
id 0
Ethernet II, Src: Intel_ff:60:4f (08:6a:c5:ff:60:4f), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
Internet Protocol Version 4, Src: 172.25.158.176, 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: 586
    Identification: 0x0276 (630)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 172.25.158.176
    Destination Address: 128.119.245.12
Transmission Control Protocol, Src Port: 10632, Dst Port: 80, Seq: 1, Ack: 1, Len: 546
    Source Port: 10632
    Destination Port: 80
    [Stream index: 111]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 546]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 2374350599
    [Next Sequence Number: 547    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
```

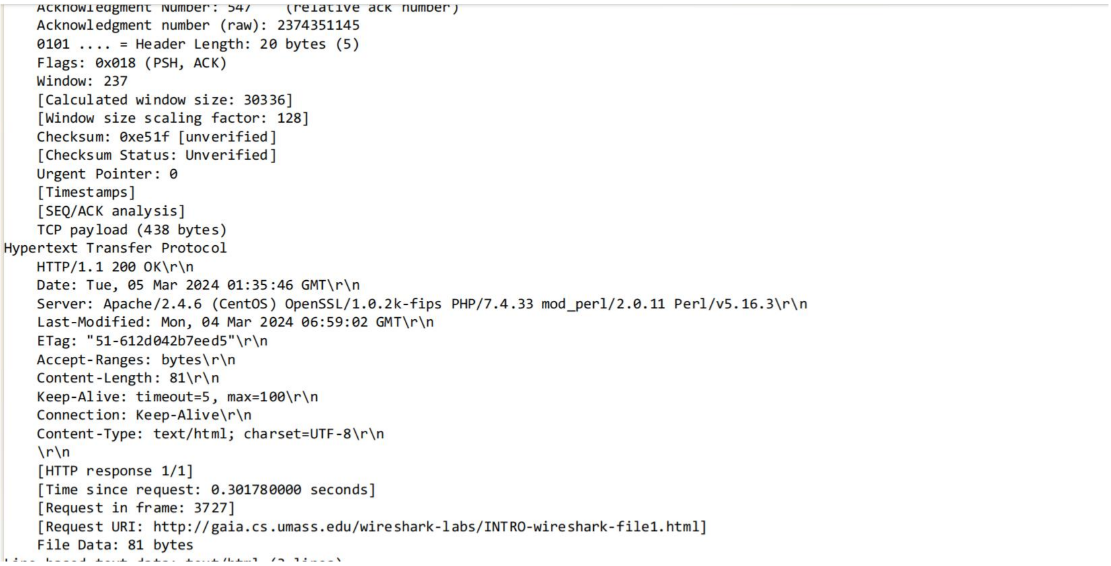


```
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3415338440
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 513
    [Calculated window size: 131328]
    [Window size scaling factor: 256]
    Checksum: 0xc28a [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
    [SEQ/ACK analysis]
    TCP payload (546 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
    Cache-Control: max-age=0\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 Edg/
122.0.0.0\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: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
    \r\n
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    [HTTP request 1/1]
    [Response in frame: 3736]
```

打印 ok



```
No.     Time           Source                Destination           Protocol Length Info
   3736 61.441760      128.119.245.12        172.25.158.176        HTTP     492    HTTP/1.1 200 OK  (text/html)
Frame 3736: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{8189733E-4FB8-456C-AD96-3C31CC679B08},
id 0
Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: Intel_ff:60:4f (08:6a:c5:ff:60:4f)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.25.158.176
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 478
    Identification: 0x1cb1 (7345)
    010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 42
    Protocol: TCP (6)
    Header Checksum: 0x721b [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 172.25.158.176
Transmission Control Protocol, Src Port: 80, Dst Port: 10632, Seq: 1, Ack: 547, Len: 438
    Source Port: 80
    Destination Port: 10632
    [Stream index: 111]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 438]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 3415338440
    [Next Sequence Number: 439    (relative sequence number)]
```



```
    Acknowledgment Number: 547    (relative ack number)
    Acknowledgment number (raw): 2374351145
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
    Window: 237
    [Calculated window size: 30336]
    [Window size scaling factor: 128]
    Checksum: 0xe51f [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: Tue, 05 Mar 2024 01:35:46 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: Mon, 04 Mar 2024 06:59:02 GMT\r\n
    ETag: "51-612d042b7eed5"\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 1/1]
    [Time since request: 0.301780000 seconds]
    [Request in frame: 3727]
    [Request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
    File Data: 81 bytes
```

**结论：**

WLAN 在不断地发送信息。

抓包捕获可以查看具体信息，包括使用的协议，接收地址，源地址，响应时间等等。