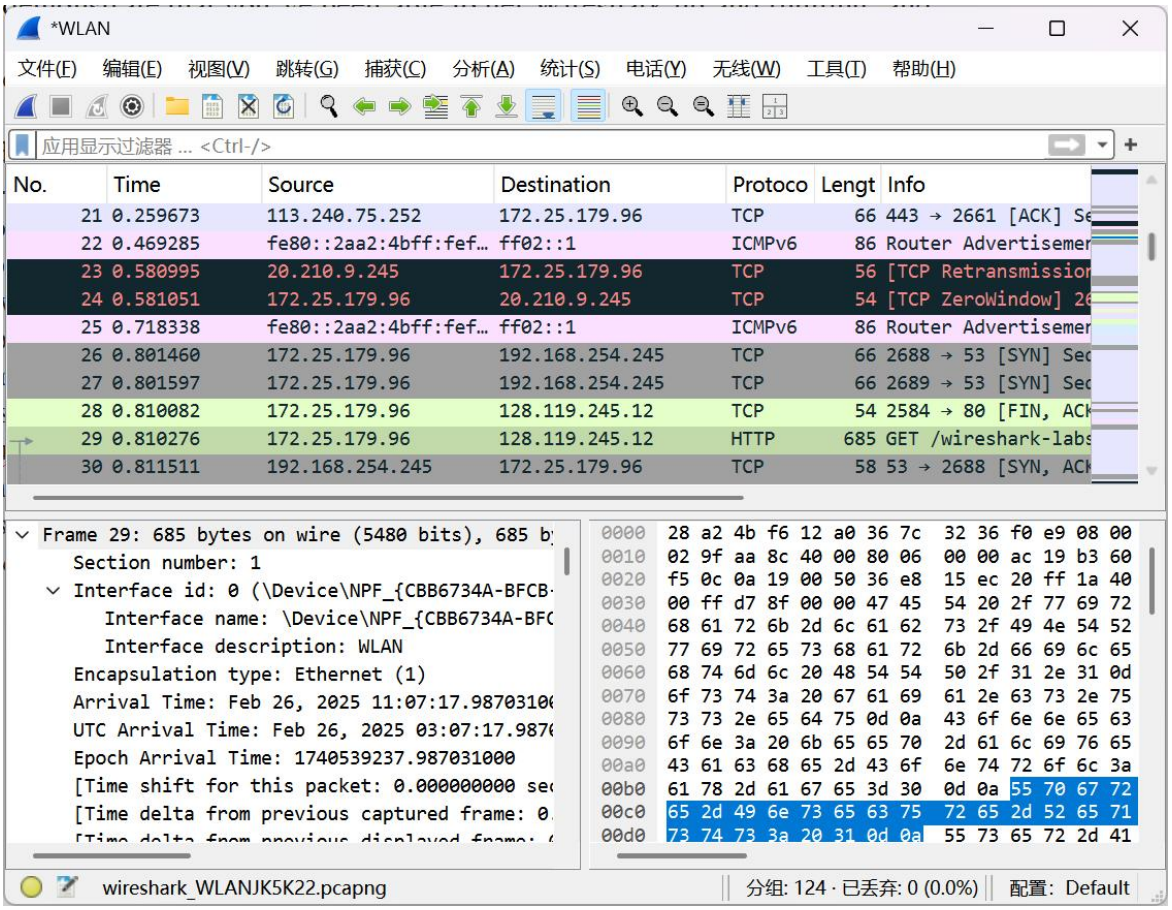
山东大学 计算机科学与技术 学院

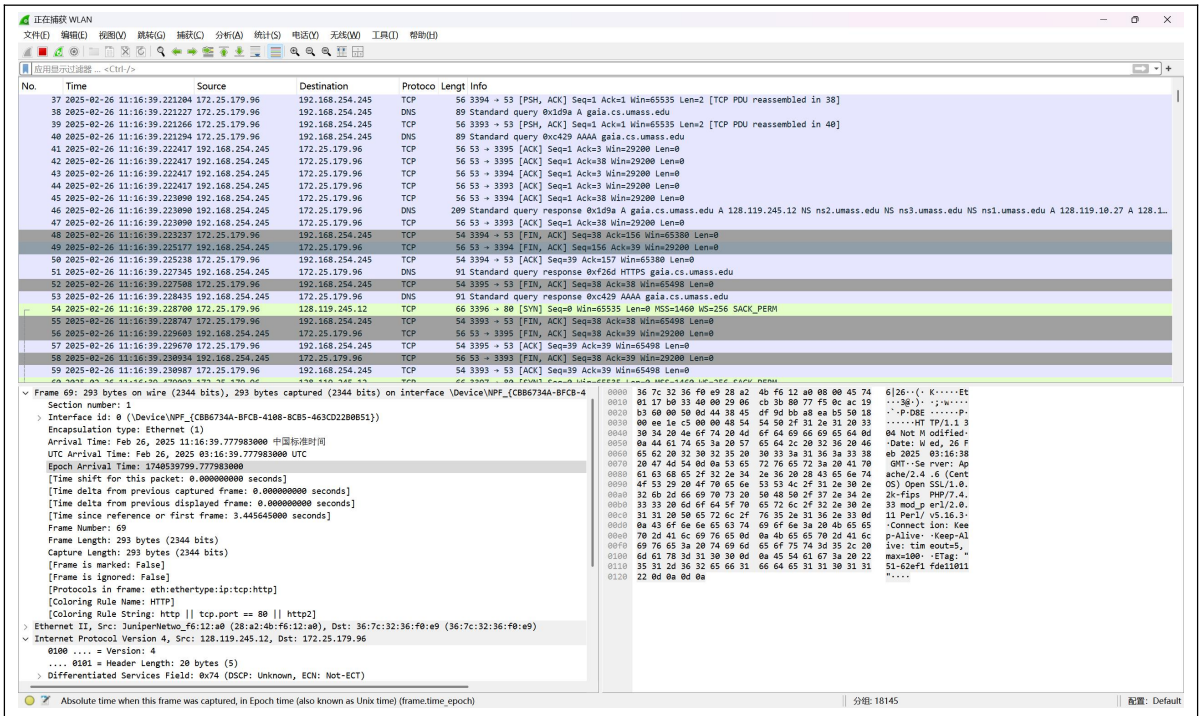
新兴网络技术与实践 课程实验报告

学号：202300130183	姓名：宋浩宇	班级：23 级智能班
实验题目：Wireshark_Intro		
实验学时：2	实验日期：2025/	
实验目的：学习使用 Wireshark		

实验结果：

1. List 3 different protocols that appear in the protocol column in the unfiltered packet-listing window in step 7 above.



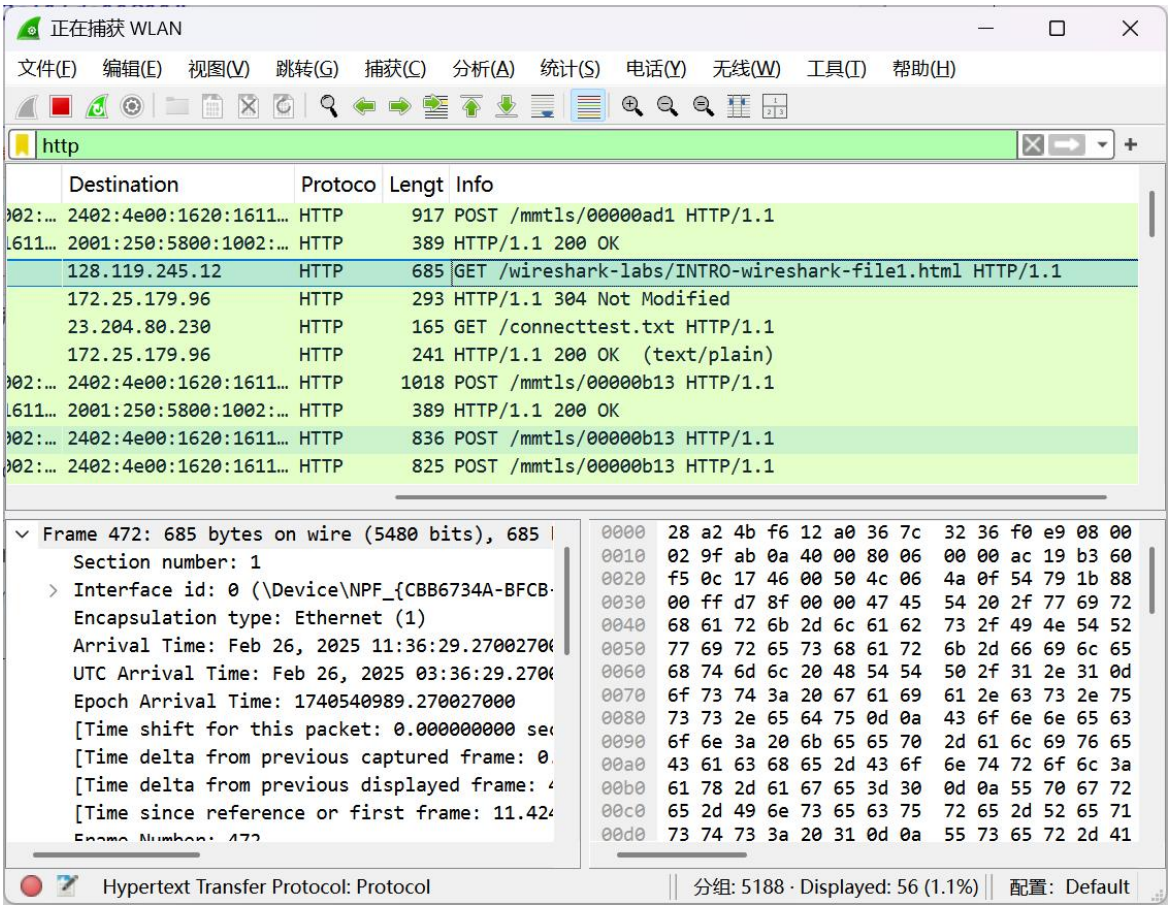


如上图所示，其中还有 TCP、ICMPv6、DNS 协议。

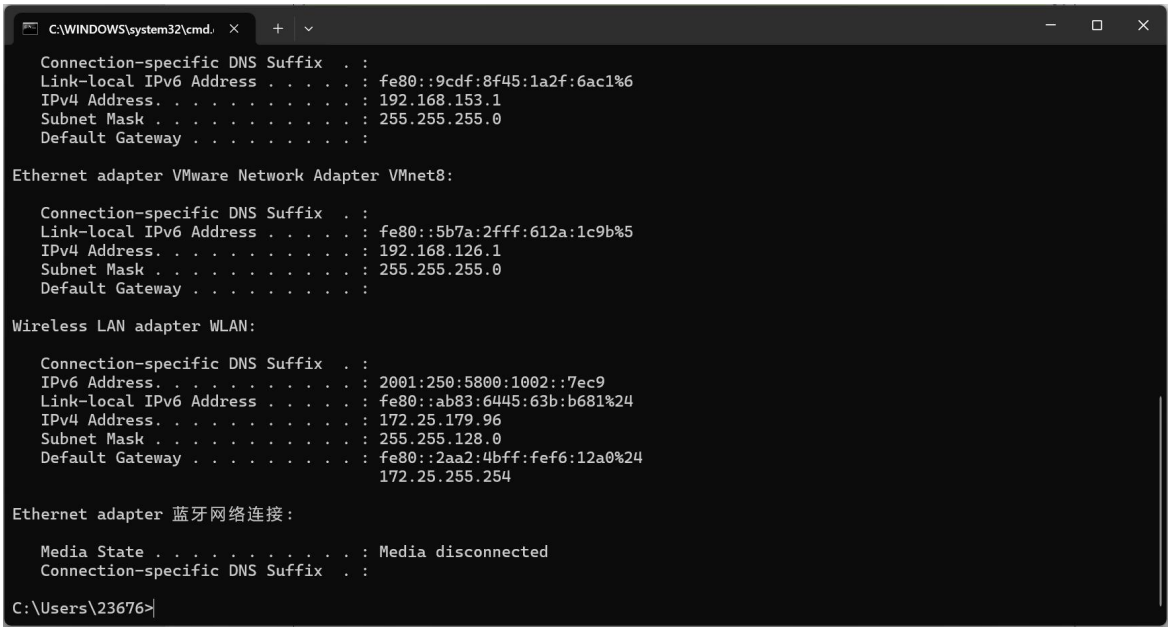
2. How long did it take from when the HTTP GET message was sent until the HTTP OK reply was received? (By default, the value of the Time column in the packet-listing window is the amount of time, in seconds, since Wireshark tracing began. To display the Time field in time-of-day format, select the Wireshark View pull down menu, then select Time Display Format, then select Time-of-day.)

如上图所示，可以通过计算客户端发出和接收到数据的时间来获取，由于使用的浏览器（edge）的安全设置的问题，我们无法控制浏览器对 http 协议链接的重定向操作，因此我们采取进行刷新操作时 not modified（304）返回的时间来作为返回 http ok（200）的时间，按照以上信息我们可以得出结果：时间为 0.601344 秒

3. What is the Internet address of the gaia.cs.umass.edu (also known as www-net.cs.umass.edu)? What is the Internet address of your computer?



根据获取的数据包中 Destination 这一项属性，我们可以知道 gaia.cs.umass.edu 的 IP 为 128.119.245.12（ipv4）



而根据我们使用的 windows 提供的 ipconfig 命令我们可以获取到本机入网 ip 为 172.25.179.96（ipv4）

2001:250:5800:1002::7ec9（ipv6）

4. Print the two HTTP messages (GET and OK) referred to in question 2 above. To do so, select Print from the Wireshark File command menu, and select the “Selected Packet Only” and “Print as

displayed" radial buttons, and then click OK.
根据提示操作我们成功将需要的信息打印出来。
下为请求信息：

```
No.     Time                           Source                Destination           Protocol Length Info
    472 2025-02-26 11:36:29.270027     172.25.179.96         128.119.245.12        HTTP     685    GET /wireshark-labs/INTRO-wireshark-
file1.html HTTP/1.1
Frame 472: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits) on interface \Device\NPF_{CBB6734A-
BFCB-4108-8CB5-463CD22B0B51}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0B51})
        Interface name: \Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0B51}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2025 11:36:29.270027000 中国标准时间
    UTC Arrival Time: Feb 26, 2025 03:36:29.270027000 UTC
    Epoch Arrival Time: 1740540989.270027000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000196000 seconds]
    [Time delta from previous displayed frame: 4.906510000 seconds]
    [Time since reference or first frame: 11.424615000 seconds]
    Frame Number: 472
    Frame Length: 685 bytes (5480 bits)
    Capture Length: 685 bytes (5480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: 36:7c:32:36:f0:e9 (36:7c:32:36:f0:e9), Dst: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
    Destination: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: 36:7c:32:36:f0:e9 (36:7c:32:36:f0:e9)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 172.25.179.96, Dst: 128.119.245.12
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 671
    Identification: 0xab0a (43786)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...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: 172.25.179.96
    Destination Address: 128.119.245.12
    [Stream index: 14]
Transmission Control Protocol, Src Port: 5958, Dst Port: 80, Seq: 1, Ack: 1, Len: 631
    Source Port: 5958
    Destination Port: 80
    [Stream index: 37]
    [Stream Packet Number: 4]
    [Conversation completeness: Complete, WITH_DATA (31)]
        ..0. .... = RST: Absent
        ...1 .... = FIN: Present
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ·FDASS]
    [TCP Segment Len: 631]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1275480591
    [Next Sequence Number: 632    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 1417223048
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····AP···]
    Window: 255
```

```
    [Calculated window size: 65280]
    [Window size scaling factor: 256]
    Checksum: 0xd78f [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.267776000 seconds]
        [Time since previous frame in this TCP stream: 0.000196000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.267580000 seconds]
        [Bytes in flight: 631]
        [Bytes sent since last PSH flag: 631]
    TCP payload (631 bytes)
Hypertext Transfer Protocol
    GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1\r\n
        Request Method: GET
        Request URI: /wireshark-labs/INTRO-wireshark-file1.html
        Request Version: HTTP/1.1
    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/133.0.0.0 Safari/537.36 Edg/
133.0.0.0\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
    If-None-Match: "51-62ef1fde11011"\r\n
    If-Modified-Since: Tue, 25 Feb 2025 06:59:01 GMT\r\n
    \r\n
    [Response in frame: 479]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```


下为返回信息:

```
No.     Time                           Source                Destination           Protocol Length Info
    479 2025-02-26 11:36:29.871371     128.119.245.12        172.25.179.96         HTTP     293    HTTP/1.1 304 Not Modified
Frame 479: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{CBB6734A-
BFCB-4108-8CB5-463CD22B0B51}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0B51})
        Interface name: \Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0B51}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 26, 2025 11:36:29.871371000 中国标准时间
    UTC Arrival Time: Feb 26, 2025 03:36:29.871371000 UTC
    Epoch Arrival Time: 1740540989.871371000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.235809000 seconds]
    [Time delta from previous displayed frame: 0.601344000 seconds]
    [Time since reference or first frame: 12.025959000 seconds]
    Frame Number: 479
    Frame Length: 293 bytes (2344 bits)
    Capture Length: 293 bytes (2344 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0), Dst: 36:7c:32:36:f0:e9 (36:7c:32:36:f0:e9)
    Destination: 36:7c:32:36:f0:e9 (36:7c:32:36:f0:e9)
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: JuniperNetwo_f6:12:a0 (28:a2:4b:f6:12:a0)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.25.179.96
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x74 (DSCP: Unknown, ECN: Not-ECT)
        0111 01.. = Differentiated Services Codepoint: Unknown (29)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable T anspo t (0)
    Total Length: 279
    Identification: 0x8cb7 (36023)
    010. .... = Flags: 0x2, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 40
    Protocol: TCP (6)
    Header Checksum: 0xefb7 [validatio  dis  ied,
    [Header checksum status: Unverified]
    Source Address: 128.119.245.12
    Destination Address: 172.25.179.96
    [Stream index: 14]
Transmission Control Protocol, Src Port: 80,  st Port: 5958, Seq: 1, Ack: 632, Len: 239
    Source Port: 80
    Destination Port: 5958
    [Stream index: 37]
    [Stream Packet Number: 6]
    [Conversation completeness: Complete, WITH_DATA (31)]
        ..0. .... = RST: Absent
        ...1 .... = FIN: Present
        .... 1... = Data: Present
        .... .1.. = ACK: Present
        .... ..1. = SYN-ACK: Present
        .... ...1 = SYN: Present
        [Completeness Flags: ·FDASS]
    [TCP Segment Len: 239]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 1417223048
    [Next Sequence Number: 240    (relative sequence number)]
    Acknowledgment Number: 632    (relative ack number)
    Acknowledgment number (raw): 1275481222
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x018 (PSH, ACK)
        000. .... .... = Reserved: Not set
        ...0 .... .... = Accurate ECN: Not set
        .... 0... .... = Congestion Window Reduced: Not set
        .... .0.. .... = ECN-Echo: Not set
        .... ..0. .... = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: ·····AP···]
    Window: 238
    [Calculated window size: 30464]
```

```
    [Window size scaling factor: 128]
    Checksum: 0xcb73 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
    [Timestamps]
        [Time since first frame in this TCP stream: 0.869120000 seconds]
        [Time since previous frame in this TCP stream: 0.333698000 seconds]
    [SEQ/ACK analysis]
        [iRTT: 0.267580000 seconds]
        [Bytes in flight: 239]
        [Bytes sent since last PSH flag: 239]
    TCP payload (239 bytes)
Hypertext Transfer Protocol
    HTTP/1.1 304 Not Modified\r\n
        Response Version: HTTP/1.1
        Status Code: 304
        [Status Code Description: Not Modified]
        Response Phrase: Not Modified
    Date: Wed, 26 Feb 2025 03:36:29 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
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    ETag: "51-62ef1fde11011"\r\n
    \r\n
    [Request in frame: 472]
    [Time since request: 0.601344000 seconds]
    [Request URI: /wireshark-labs/INTRO-wireshark-file1.html]
    [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html]
```

问题及收获：

主要问题在于实验指导书给出的测试链接使用的为 http 协议，而因为现代大部分网站使用的是 https 协议，因此浏览器（edge）认为这个链接是不安全的，这导致了在浏览器中打开这个链接是会被不可控的重定向，且 Microsoft 并没有给我们提供任何途径可以禁用浏览器的这个功能，因此在尝试获取 http 请求和 http OK 时会失败，但经过测试再进行刷新操作时浏览器并不会屏蔽 http 协议的请求和返回，因此实验报告部分的截图均来自刷新过程获取的数据。