

新兴网络技术与实践 课程实验报告

1 / 9

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

应用显示过滤器: <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
37	2025-02-26 11:16:39.221284	172.25.179.96	192.168.254.245	TCP	56	3394 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=2 [TCP PDU reassembled in 38]
38	2025-02-26 11:16:39.221227	172.25.179.96	192.168.254.245	DNS	89	Standard query 0x1d9a A gaia.cs.umass.edu
39	2025-02-26 11:16:39.221266	172.25.179.96	192.168.254.245	TCP	56	3393 → 53 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=2 [TCP PDU reassembled in 40]
40	2025-02-26 11:16:39.221294	172.25.179.96	192.168.254.245	DNS	89	Standard query 0xc429 AAAA gaia.cs.umass.edu
41	2025-02-26 11:16:39.222417	192.168.254.245	172.25.179.96	TCP	56	53 → 3395 [ACK] Seq=1 Ack=3 Win=29200 Len=0
42	2025-02-26 11:16:39.222417	192.168.254.245	172.25.179.96	TCP	56	53 → 3395 [ACK] Seq=1 Ack=3 Win=29200 Len=0
43	2025-02-26 11:16:39.222417	192.168.254.245	172.25.179.96	TCP	56	53 → 3394 [ACK] Seq=1 Ack=3 Win=29200 Len=0
44	2025-02-26 11:16:39.222417	192.168.254.245	172.25.179.96	TCP	56	53 → 3393 [ACK] Seq=1 Ack=3 Win=29200 Len=0
45	2025-02-26 11:16:39.223890	192.168.254.245	172.25.179.96	TCP	56	53 → 3394 [ACK] Seq=1 Ack=3 Win=29200 Len=0
46	2025-02-26 11:16:39.223890	192.168.254.245	172.25.179.96	DNS	289	Standard query response 0x1d9a A gaia.cs.umass.edu A 128.119.245.12 NS ns2.umass.edu NS ns3.umass.edu NS ns1.umass.edu A 128.119.18.27 A 128.11.16.1
47	2025-02-26 11:16:39.223890	192.168.254.245	172.25.179.96	TCP	56	53 → 3393 [ACK] Seq=1 Ack=3 Win=29200 Len=0
48	2025-02-26 11:16:39.223237	172.25.179.96	192.168.254.245	TCP	54	3394 → 53 [FIN, ACK] Seq=38 Ack=156 Win=65380 Len=0
49	2025-02-26 11:16:39.225177	192.168.254.245	172.25.179.96	TCP	56	53 → 3394 [FIN, ACK] Seq=156 Ack=39 Win=29200 Len=0
50	2025-02-26 11:16:39.225238	172.25.179.96	192.168.254.245	TCP	54	3394 → 53 [ACK] Seq=39 Ack=157 Win=65380 Len=0
51	2025-02-26 11:16:39.227340	192.168.254.245	172.25.179.96	DNS	91	Standard query response 0x126d HTTPS gaia.cs.umass.edu
52	2025-02-26 11:16:39.227588	172.25.179.96	192.168.254.245	TCP	54	3395 → 53 [FIN, ACK] Seq=38 Ack=38 Win=65498 Len=0
53	2025-02-26 11:16:39.228435	192.168.254.245	172.25.179.96	DNS	91	Standard query response 0xc429 AAAA gaia.cs.umass.edu
54	2025-02-26 11:16:39.228780	172.25.179.96	128.119.245.12	TCP	66	3396 → 80 [SYN] Seq=0 Win=65535 Len=0 MSG=1460 WS=256 SACK_PERM
55	2025-02-26 11:16:39.228787	172.25.179.96	192.168.254.245	TCP	54	3393 → 53 [FIN, ACK] Seq=38 Ack=38 Win=65498 Len=0
56	2025-02-26 11:16:39.229603	192.168.254.245	172.25.179.96	TCP	56	53 → 3395 [FIN, ACK] Seq=38 Ack=39 Win=29200 Len=0
57	2025-02-26 11:16:39.229670	172.25.179.96	192.168.254.245	TCP	54	3395 → 53 [ACK] Seq=39 Ack=39 Win=65498 Len=0
58	2025-02-26 11:16:39.230934	192.168.254.245	172.25.179.96	TCP	56	53 → 3393 [FIN, ACK] Seq=38 Ack=39 Win=29200 Len=0
59	2025-02-26 11:16:39.230987	172.25.179.96	192.168.254.245	TCP	54	3393 → 53 [ACK] Seq=39 Ack=39 Win=65498 Len=0

▼ Frame 69: 293 bytes on wire (2344 bits), 293 bytes captured (2344 bits) on interface \Device\NPF_{C8B6734A-BFCB-4108-8C85-465CD22B0B51} [eth0]

Section number: 1

Interface Id: 0 (\Device\NPF_{C8B6734A-BFCB-4108-8C85-465CD22B0B51})

Encapsulation type: Ethernet II

Arrival Time: Feb 26, 2025 11:16:39.777983000 中国标准时间

UTC Arrival Time: Feb 26, 2025 03:16:39.777983000 UTC

Epoch Arrival Time: 1748539799.777983000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 3.445645000 seconds]

Frame Number: 69

Frame Length: 293 bytes (2344 bits)

Capture Length: 293 bytes (2344 bits)

[Frame is marked: False]

[Frame is ignored: False]

Protocols in frame: ethertype:ip:tcp:http

[Coloring Rule Name: HTTP]

[Coloring Rule String: http || tcp.port == 80 || http2]

▼ Ethernet II, Src: JuniperNetwo_76:12:a8 (28:a2:40:f6:12:a8), Dst: 36:7c:32:36:f0:e9 (36:7c:32:36:f0:e9)

▼ 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)

0000 36 7c 32 36 f0 e9 28 a2 40 f6 12 a0 08 00 45 74 6126...K.....Et

0010 01 17 00 33 40 00 29 86 c0 3b 80 77 f5 0c ac 19 ...80...;w....

0020 53 00 00 50 bd 44 38 45 ff fd b0 a0 ea b5 18 1b ...P...P.....P

0030 00 ee 1e c5 00 00 48 54 54 50 2f 31 20 31 20 33HT TP/1.3

0040 30 20 4e ff 74 20 4d 6f 64 69 66 69 65 64 60 60 04 Not Modified

0050 0a 44 61 74 65 3a 20 57 65 64 2c 20 32 36 20 46 -Date: Wed, 26 F

0060 65 62 20 32 30 32 35 20 30 33 3a 31 36 3a 33 38 eb 2025 03:16:38

0070 20 47 4d 54 8d 0a 53 65 72 76 65 72 3a 20 41 70 GMT -Se rven: Ap

0080 61 63 68 65 2f 32 2e 34 2e 36 20 28 43 65 6a 74 ache/2.4.6 (Cent

0090 4f 53 29 20 4f 70 65 6e 53 53 4c 2f 31 2a 30 2a 05) Open SSL/1.0.

00a0 32 6b 26 66 69 70 73 20 50 48 80 2f 37 2a 3a 2e 3x-fips PMP/7.4.

00b0 33 33 20 6d 6f 64 5f 70 65 72 6c 2f 32 2a 30 2e 33 mod_perl/2.0.

00c0 31 31 20 50 65 72 6c 2f 76 55 2e 31 36 2a 33 6d 11 Perl/ v5.16.3.

00d0 0a 43 6f 6e 65 63 74 69 6f 6a 3a 20 4b 65 65 -Connect ion: Kee

00e0 70 2d 41 6c 69 76 65 6d 0a 4b 65 65 70 2d 41 6c p-Alive -Keep-Al

00f0 69 76 65 3a 20 74 69 6d 65 6f 75 74 3a 35 2c 20 live: tim out=5.

0100 6d 67 3d 31 30 30 6d 0a 45 54 61 67 3a 20 22 max=100 -ETag:

0110 35 31 2d 36 32 65 66 31 66 64 65 31 31 30 31 31 51-6zeP1 fde11011

0120 2d 6d 0a 6d 6a

Absolute time when this frame was captured, in Epoch time (also known as Unix time) (frame.time_epoch)

分组: 18145

配置: Default

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.)

2 / 9

Wireshark · 追踪 HTTP 流 (tcp.stream eq 37) · WLAN

GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Host: gaia.cs.umass.edu

Connection: keep-alive

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

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

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

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6

If-None-Match: "51-62ef1fde11011"

If-Modified-Since: Tue, 25 Feb 2025 06:59:01 GMT

HTTP/1.1 304 Not Modified

Date: Wed, 26 Feb 2025 03:36:29 GMT

Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.33 mod_perl/2.0.11 Perl/v5.16.3

Connection: Keep-Alive

Keep-Alive: timeout=5, max=100

ETag: "51-62ef1fde11011"

分组 479。1 客户端 分组, 1 服务器 分组, 1 turn(s).点击选择。

整个对话 (870 bytes)

显示为 ASCII

No delta times

流 37

查找:

☐ 区分大小写

查找下一个(N)

滤掉此流

打印

另存为...

返回

关闭

帮助

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?

3 / 9

正在捕获 WLAN

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
470	0.000000	2402:4e00:1620:1611::...	2402:4e00:1620:1611::...	HTTP	917	POST /mmtls/00000ad1 HTTP/1.1
471	0.000000	2001:250:5800:1002::...	2001:250:5800:1002::...	HTTP	389	HTTP/1.1 200 OK
472	0.000000	128.119.245.12	172.25.179.96	HTTP	685	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
473	0.000000	172.25.179.96	172.25.179.96	HTTP	293	HTTP/1.1 304 Not Modified
474	0.000000	23.204.80.230	172.25.179.96	HTTP	165	GET /connecttest.txt HTTP/1.1
475	0.000000	172.25.179.96	172.25.179.96	HTTP	241	HTTP/1.1 200 OK (text/plain)
476	0.000000	2402:4e00:1620:1611::...	2402:4e00:1620:1611::...	HTTP	1018	POST /mmtls/00000b13 HTTP/1.1
477	0.000000	2001:250:5800:1002::...	2001:250:5800:1002::...	HTTP	389	HTTP/1.1 200 OK
478	0.000000	2402:4e00:1620:1611::...	2402:4e00:1620:1611::...	HTTP	836	POST /mmtls/00000b13 HTTP/1.1
479	0.000000	2402:4e00:1620:1611::...	2402:4e00:1620:1611::...	HTTP	825	POST /mmtls/00000b13 HTTP/1.1

Frame 472: 685 bytes on wire (5480 bits), 685 bytes captured (5480 bits) on interface 0 (\\Device\\NPF_{CBB6734A-BFCB-4A0F-5479-1B88-000000000000})

Section number: 1

Interface id: 0 (\\Device\\NPF_{CBB6734A-BFCB-4A0F-5479-1B88-000000000000})

Encapsulation type: Ethernet (1)

Arrival Time: Feb 26, 2025 11:36:29.270027000

UTC Arrival Time: Feb 26, 2025 03:36:29.270027000

Epoch Arrival Time: 1740540989.270027000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 11.420000000 seconds]

Frame Number: 472

Hypertext Transfer Protocol: Protocol

分组: 5188 · Displayed: 56 (1.1%) 配置: Default

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)

```
C:\WINDOWS\system32\cmd. x + v
Connection-specific DNS Suffix . :
Link-Local IPv6 Address . . . . . : fe80::9cdf:8f45:1a2f:6ac1%6
IPv4 Address. . . . . : 192.168.153.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

Connection-specific DNS Suffix . :
Link-Local IPv6 Address . . . . . : fe80::5b7a:2fff:612a:1c9b%5
IPv4 Address. . . . . : 192.168.126.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :

Wireless LAN adapter WLAN:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:250:5800:1002::7ec9
Link-Local IPv6 Address . . . . . : fe80::ab83:6445:63b:b681%24
IPv4 Address. . . . . : 172.25.179.96
Subnet Mask . . . . . : 255.255.128.0
Default Gateway . . . . . : fe80::2aa2:4bff:fef6:12a0%24
172.25.255.254

Ethernet adapter 蓝牙网络连接:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\23676>
```

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
      ....1.. = Reset: Not set
      ....1. .... = Syn: Not set
      ....1.. = 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-4108-8CB5-463CD22B0851}, id 0
BFCB-4108-8CB5-463CD22B0851, id 0

Section number: 1

Interface id: 0 (\Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0851})
Interface name: \Device\NPF_{CBB6734A-BFCB-4108-8CB5-463CD22B0851}
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 Transport (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 [validation disabled]
[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, Dst 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]
```

试用水印

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。