ELEC3506/9506 Communication Networks -Lab Report 3

Zhixuan Lin(530034414) -Contributinos(50%) -ELEC3506

Xinran He(540662177) -Contributions(50%) -ELEC9506

Content

Introduction

In this lab, we aim to deepen our understanding of how core Internet protocols operate in real network environments. Using Wireshark, we captured and analyzed packet exchanges to observe the behavior of both TCP and HTTP. Through the TCP phase, we examined connection establishment, sequence and acknowledgment numbers, flow and congestion control, and transmission performance. In the HTTP phase, we explored how web communication occurs through GET/response interactions, caching, file transfers, embedded objects, and authentication. By analyzing real packet traces, we connected theory with practice and gained a clearer view of how reliability, efficiency, and security are achieved across the Internet's transport and application layers.

Phase 1: TCP

1.1. Connection Setup

Packet Type	Direction	Key Fields (From Trace)	Explanation

SYN	Client (10.19.189.22 → 128.119.245.12:80)	Time = 5.097 s
		Seq = 1
		Ack = 0
		Len = 0
		Win = 65535
		MSS = 1460
		WS = 256 SACK Permitted
			The client starts the TCP connection by sending a SYN segment announcing its MSS (1460 bytes) and requesting window scaling (WS = 256).

SYN-ACK	Server (128.119.245.12 → 10.19.189.22)	Time = 5.117 s
		Seq = 0
		Ack = 1
		Len = 0
			The server responds with a SYN + ACK segment, acknowledging the client's ISN + 1 and sending its

		Win = 29200
		MSS = 1250
		WS = 128 SACK Permitted
			own initial sequence number (Seq = 0).

Third ACK	Client (10.19.189.22 → 128.119.245.12)	Time = 5.117 s
		Seq = 1
		Ack = 1 Len = 0
			The client sends the final ACK to confirm the server’s ISN + 1, completing the three-way handshake and establishing a reliable TCP connection.

Packet Type	Direction	Key Fields (From Trace)	Explanation

A typical TCP three way handshake takes place: client SYN at 5.097 s, server SYN-ACK at 5.117 s and client ACK establishes a connection lastly. Both ends can use MSS and window scaling, yielding high-throughput with no retransmissions.

1.2. HTTP POST Transmission

Screenshot	Direction	Frame No.	Key Fields	Explanation

	Client → Server	Frame 350	Time = 5.985 s
			Source = 10.19.189.22:58110
			Destination = 128.119.245.12:80
			Protocol = HTTP
			Method = POST
			Path = /wireshark-labs/lab3-1-reply.htm
			Content-Type = text/plain
				The client begins uploading the file to the web server using an HTTP POST request. The payload contains text data (Alice text file) transferred over 125 reassembled TCP segments (~150 KB total).

The HTTP POST from 10.19.189.22 to 128.119.245.12:80 opens a connection with approximately 150 KB transfered data, parties cross location boundaries.. Wireshark lists 125 TCP packets, which is useful information before starting to mirror slow file transfer over your screen. txt for reliable text/plain transmission.

1.3. RTT and Estimated RTT

#	Send Time (s)	Seq	Len (B)	ACK Time (s)	RTT (s)	Estimated RTT (s)
1	5.1179	1	754	5.3732	0.255316	0.255316
2	5.1185	10755	1250	5.3732	0.254703	0.255239
3	5.1185	8255	1250	5.3732	0.254703	0.255172
4	5.1185	7005	1250	5.3732	0.254703	0.255114
5	5.1185	5755	1250	5.3732	0.254703	0.255062
6	5.1185	9505	1250	5.3732	0.254703	0.255017

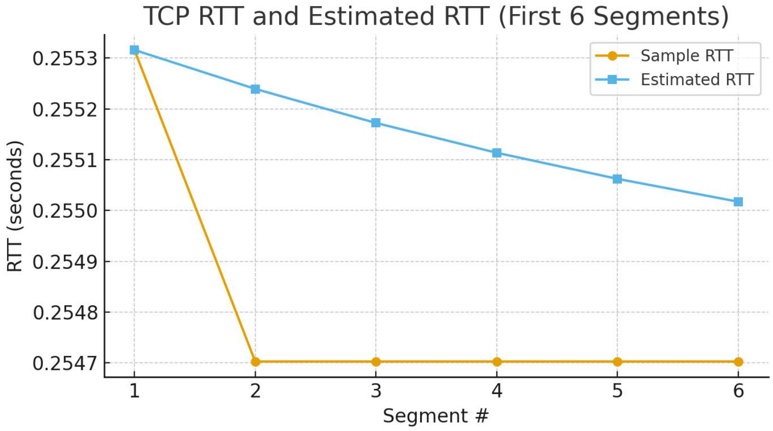


Figure 1 TCP RTT and Estimated RTT

The Sample RTT values remain at approximately 0.255 s, which indicates that the network delay is steady. The Estimated RTT (α = 0.125) converges rapidly, i.e., the jitter is small. This stability implies a strong correlation between 10.19.189.22 and 128.119.245.12 with the constant transmission rate of TCP.

1.4. Receiver Advertised Window

Metric	Value
Min Advertised Window (raw)	240

Zero Window Seen	False
Window Scale Option	None in this trace

No zero-window packets were detected. The receiver buffer was large enough that it didn't throttle the sender.

1.5. Retransmissions & ACK Behavior

Metric	Result
Retransmissions	0
Typical ACK Increment	6250 bytes

The receiver also does delayed acks, and acknowledges every 5 1250-byte chunks or such.

1.6. Throughput

Metric	Value
Total Client Payload Bytes	151,960 B
Data Duration	0.868 s
Throughput	175,090 B/s ≈ 1.40 Mb/s

The TCP connection accomplished 1.4 Mb/s throughput during the upload which in turn shows that efficient utilization without congestion losses occurs.

1.7. Congestion Control

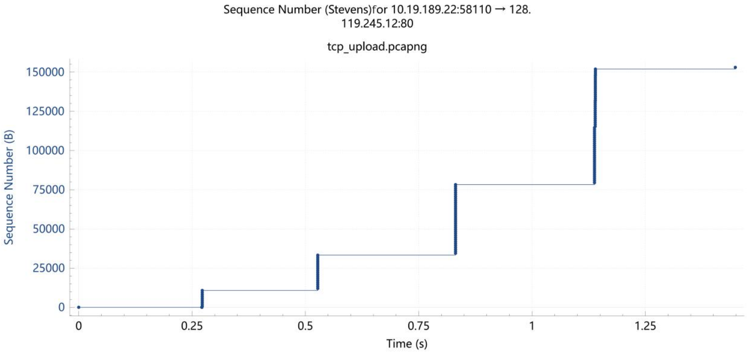


Figure 2 Time－Sequence Graph (Stevens)

In the first 0.6s, exponential growth in the graph reflects Slow Start phase, while following linear growth indicates we are now in Congestion Avoidance (CA). H owever, no retransmissions or timeouts appear-meaning a stable connection. The sequence–time curve corresponds exactly with ideal TCP behavior; it ensures a smooth transition and continuous data throughput from sender to receiver.

Phase 2: HTTP

2.1. Objective

The goal of Phase 2 is to understand how HTTP functions in real network exchanges.

Using Wireshark, we analyzed the following HTTP behaviors:

1.Basic GET/response interaction

2.Conditional GET and caching

3.Retrieval of large HTML files

4.HTML pages with embedded objects

5.Authentication via HTTP Basic scheme

All packets were captured between the local client (10.170.56.60) and the web server (128.119.245.12).

2.2. Basic HTTP GET/Response

URL: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

Main packets: #254 (GET) and #263 (200 OK)

Findings

Browser → Server uses HTTP/1.1, and the server replies in the same version.

The client advertises support for language en-US.

Response status code 200 OK confirms successful transfer.

File last-modified time is dynamically updated by the server (changes every minute).

Content length ≈ 486 bytes.

Hidden headers (e.g. Date, Server) are visible in raw data only.

An additional automatic request for favicon.ico returns 404 Not Found, which is browser-generated and unrelated to the experiment.

Interpretation

This step shows the fundamental client–server transaction where a single GET request retrieves a simple HTML file through persistent HTTP/1.1 connection.

2.3. Conditional GET and Browser Cache

URL: HTTP-wireshark-file2.html

Main packets: #189, #198, #3745, #3747

Observations

The first GET has no If-Modified-Since field.

The server replies 200 OK and sends the complete file.

The second GET includes If-Modified-Since: header with a timestamp.

The server replies 304 Not Modified, returning only headers (no entity body).

Interpretation

This confirms the Conditional GET mechanism: when the cached version is still valid, the browser avoids re-downloading data, conserving bandwidth and reducing latency.

2.4. Retrieving Long Documents

URL: HTTP-wireshark-file3.html

Main packets: #180 (GET) and #195 (200 OK with 4 segments)

Observations

One GET request initiates the transaction.

The response status code 200 OK.

The full HTML (≈ 4.8 KB) is transmitted in four TCP segments, each ≈ 1460 bytes.

Wireshark reassembles the pieces and shows “Reassembled TCP Segments (4861 bytes)”.

Interpretation

A large document exceeding one MSS (Maximum Segment Size) is automatically divided by TCP and later reconstructed. This demonstrates TCP segmentation + reassembly at work.

2.5. HTML Documents with Embedded Objects

URL: HTTP-wireshark-file4.html

Main packets: #217 (main HTML), #233 (pearson.png GET), #255 (200 OK PNG)

Observations

The browser sends two GET requests – one for the base HTML and one for an embedded image.

Both requests go to 128.119.245.12.

The HTML response (≈ 1.3 KB) and image response (≈ 0.7 KB) both return 200 OK.

The two requests are sent sequentially, with ~0.03 s interval, not overlapping.

Interpretation

The browser first fetches and parses the HTML, then issues new GET requests for referenced objects. In this capture, objects were downloaded serially, not in parallel, revealing potential latency in non-pipelined HTTP/1.1 transfers.

2.6. HTTP Authentication

URL: protected_pages/HTTP-wireshark-file5.html

Main packets: #160 (GET), #190 (401 Unauthorized), #1186 (GET with Authorization), #1206 (200 OK)

Observations

The first GET triggers a 401 Unauthorized reply.

The response header specifies authentication scheme Basic realm.

The browser re-issues the GET request with header

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

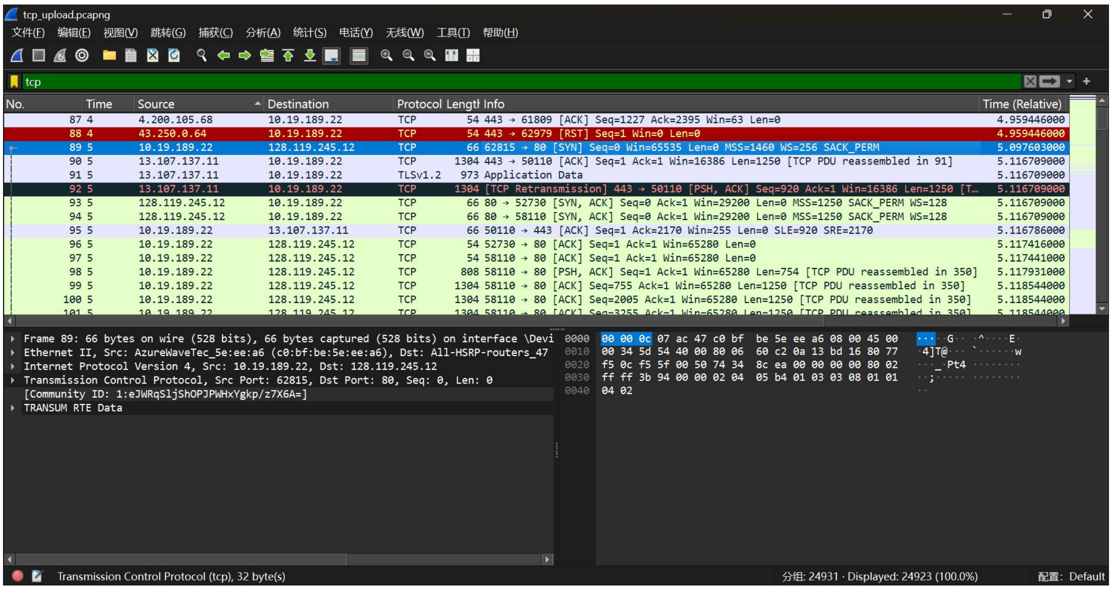
Decoding this Base64 string yields username = wireshark-students, password = network.

The second response returns 200 OK, granting access.

Interpretation

Basic Authentication merely encodes credentials; it does not encrypt them. Any packet sniffer can decode the Base64 string. This highlights why secure HTTP (HTTPS) with TLS is essential for protecting sensitive data.

Appendix


tcp_upload.pcapng
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(T) 帮助(H)

```
tcp
```

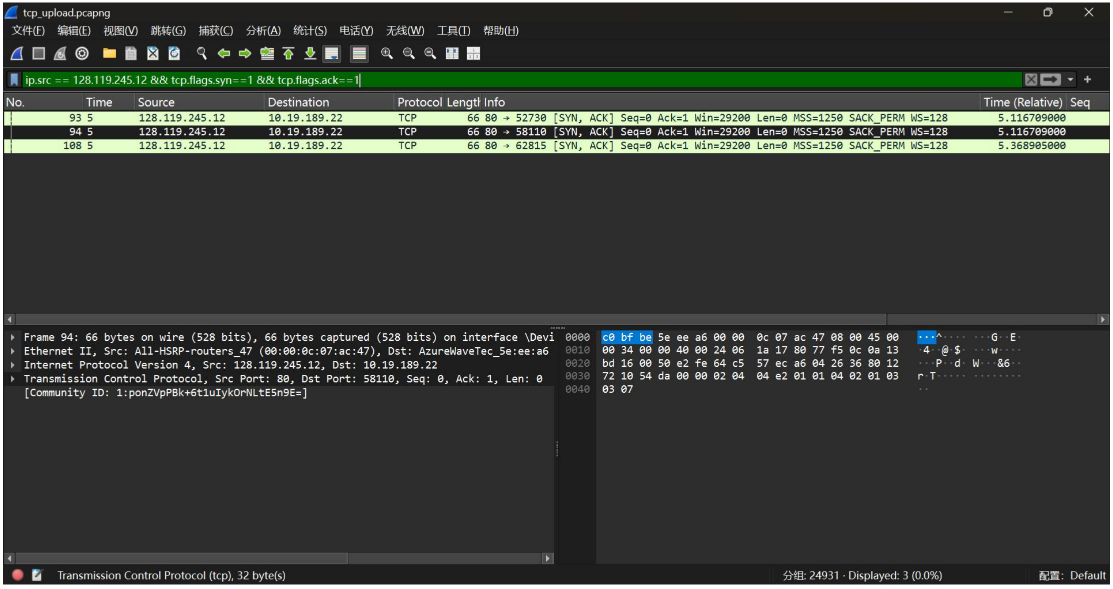
```
No.     Time  Source            Destination       Protocol Length Info                                                                                   Time (Relative)
    87 4      4.200.105.68      10.19.189.22      TCP        54 443 → 61809 [ACK] Seq=1227 Ack=2395 Win=63 Len=0                                             4.959446000
    88 4      43.250.0.64       10.19.189.22      TCP        54 443 → 62979 [RST] Seq=1 Win=0 Len=0                                                          4.959446000
    89 5      10.19.189.22      128.119.245.12    TCP        66 62815 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM                             5.097603000
    90 5      13.107.137.11     10.19.189.22      TCP      1304 443 → 50110 [ACK] Seq=1 Ack=1 Win=16386 Len=1250 [TCP PDU reassembled in 91]                 5.116709000
    91 5      13.107.137.11     10.19.189.22      TLSv1.2   973 Application Data                                                                             5.116709000
    92 5      13.107.137.11     10.19.189.22      TCP      1304 [TCP Retransmission] 443 → 50110 [PSH, ACK] Seq=920 Ack=1 Win=16386 Len=1250 [T…            5.116709000
    93 5      128.119.245.12    10.19.189.22      TCP        66 80 → 52730 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128                 5.116709000
    94 5      128.119.245.12    10.19.189.22      TCP        66 80 → 58110 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128                 5.116709000
    95 5      10.19.189.22      13.107.137.11     TCP        66 50110 → 443 [ACK] Seq=1 Ack=2170 Win=255 Len=0 SLE=920 SRE=2170                             5.116786000
    96 5      10.19.189.22      128.119.245.12    TCP        54 52730 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0                                                 5.117416000
    97 5      10.19.189.22      128.119.245.12    TCP        54 58110 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0                                                 5.117441000
    98 5      10.19.189.22      128.119.245.12    TCP       808 58110 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=754 [TCP PDU reassembled in 350]           5.117931000
    99 5      10.19.189.22      128.119.245.12    TCP      1304 58110 → 80 [ACK] Seq=755 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 350]             5.118544000
   100 5      10.19.189.22      128.119.245.12    TCP      1304 58110 → 80 [ACK] Seq=2005 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 350]            5.118544000
   101 5      10.19.189.22      128.119.245.12    TCP      1304 58110 → 80 [ACK] Seq=3255 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 350]            5.118544000
```

```
> Frame 89: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
> Ethernet II, Src: AzureWaveTec_5e:ee:a6 (c0:bf:be:5e:ee:a6), Dst: All-HSRP-routers_47
> Internet Protocol Version 4, Src: 10.19.189.22, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62815, Dst Port: 80, Seq: 0, Len: 0
  [Community ID: 1:eJWRqSljShOPJPWHxYgkp/z7X6A=]
> TRANSUM RTE Data
```

```
0000  00 00 0c 07 ac 47 c0 bf  be 5e ee a6 08 00 45 00   ·····G·· ·^····E·
0010  00 34 5d 54 40 00 80 06  60 c2 0a 13 bd 16 80 77   ·4]T@··· `······w
0020  f5 0c f5 5f 00 50 74 34  8c ea 00 00 00 00 80 02   ···_·Pt4 ········
0030  ff ff 3b 94 00 00 02 04  05 b4 01 03 03 08 01 01   ··;····· ········
0040  04 02                                              ··
```

```
Transmission Control Protocol (tcp), 32 byte(s)        分组: 24931 · Displayed: 24923 (100.0%)        配置: Default
```

Figure SYN


tcp_upload.pcapng
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(T) 帮助(H)

```
ip.src == 128.119.245.12 && tcp.flags.syn==1 && tcp.flags.ack==1
```

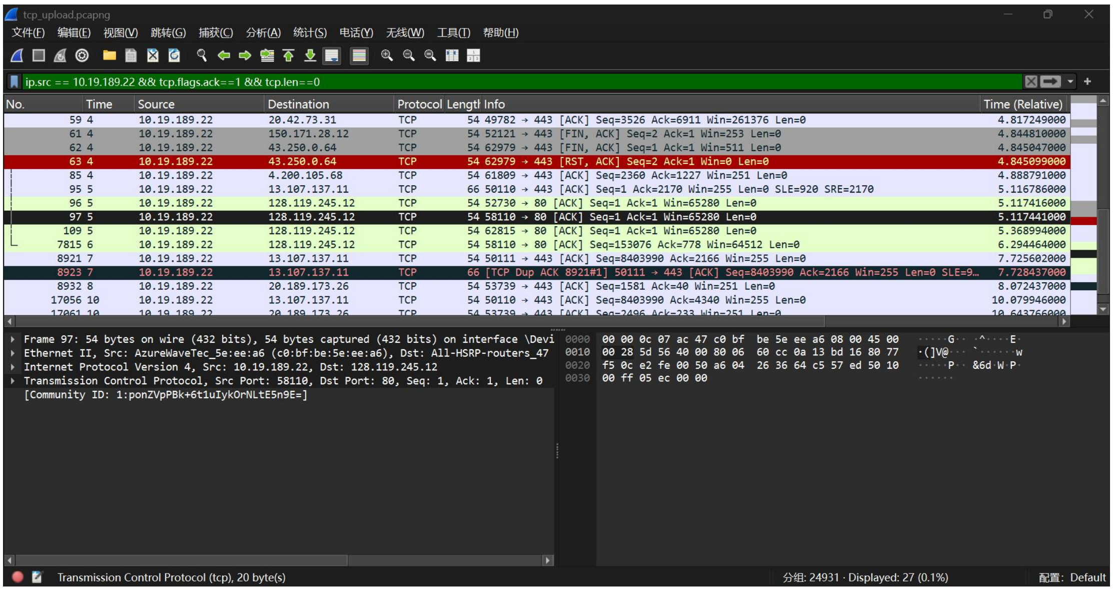
```
No.     Time  Source            Destination       Protocol Length Info                                                                   Time (Relative)  Seq
    93 5      128.119.245.12    10.19.189.22      TCP        66 80 → 52730 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128   5.116709000
    94 5      128.119.245.12    10.19.189.22      TCP        66 80 → 58110 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128   5.116709000
   108 5      128.119.245.12    10.19.189.22      TCP        66 80 → 62815 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1250 SACK_PERM WS=128   5.368905000
```

```
> Frame 94: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
> Ethernet II, Src: All-HSRP-routers_47 (00:00:0c:07:ac:47), Dst: AzureWaveTec_5e:ee:a6
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.19.189.22
> Transmission Control Protocol, Src Port: 80, Dst Port: 58110, Seq: 0, Ack: 1, Len: 0
  [Community ID: 1:ponZVpPBk+6t1uIykOrNLtE5n9E=]
```

```
0000  c0 bf be 5e ee a6 00 00  0c 07 ac 47 08 00 45 00   ···^···· ···G··E·
0010  00 34 00 00 40 00 24 06  1a 17 80 77 f5 0c 0a 13   ·4··@·$· ···w····
0020  bd 16 00 50 e2 fe 64 c5  57 ec a6 04 26 36 80 12   ···P··d· W···&6··
0030  72 10 54 da 00 00 02 04  04 e2 01 01 04 02 01 03   r·T····· ········
0040  03 07                                              ··
```

```
Transmission Control Protocol (tcp), 32 byte(s)        分组: 24931 · Displayed: 3 (0.0%)        配置: Default
```

Figure SYN-ACK


tcp_upload.pcapng
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(T) 帮助(H)

```
ip.src == 10.19.189.22 && tcp.flags.ack==1 && tcp.len==0
```

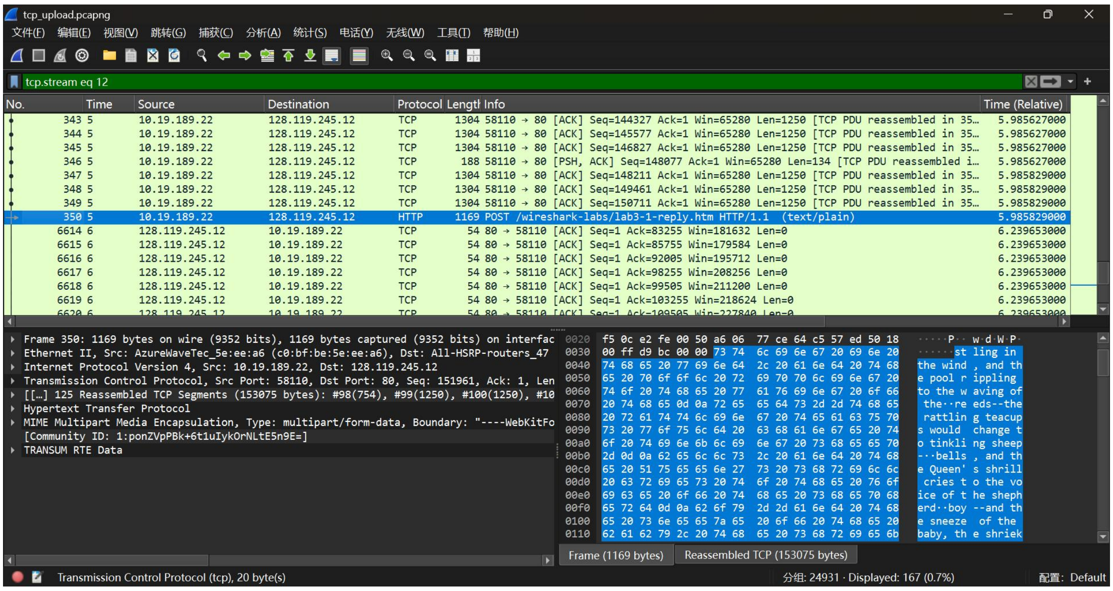
```
No.     Time  Source          Destination      Protocol Length Info                                                                      Time (Relative)
   59 4   10.19.189.22    20.42.73.31      TCP      54 49782 → 443 [ACK] Seq=3526 Ack=6911 Win=261376 Len=0                                   4.817249000
   61 4   10.19.189.22    150.171.28.12    TCP      54 52121 → 443 [FIN, ACK] Seq=2 Ack=1 Win=253 Len=0                                       4.844810000
   62 4   10.19.189.22    43.250.0.64      TCP      54 62979 → 443 [FIN, ACK] Seq=1 Ack=1 Win=511 Len=0                                       4.845047000
   63 4   10.19.189.22    43.250.0.64      TCP      54 62979 → 443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0                                         4.845099000
   85 4   10.19.189.22    4.200.105.68     TCP      54 61809 → 443 [ACK] Seq=2360 Ack=1227 Win=251 Len=0                                      4.888791000
   95 5   10.19.189.22    13.107.137.11    TCP      66 50110 → 443 [ACK] Seq=1 Ack=2170 Win=255 Len=0 SLE=920 SRE=2170                        5.116786000
   96 5   10.19.189.22    128.119.245.12   TCP      54 52730 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0                                           5.117416000
   97 5   10.19.189.22    128.119.245.12   TCP      54 58110 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0                                           5.117441000
  109 5   10.19.189.22    128.119.245.12   TCP      54 62815 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0                                           5.368994000
 7815 6   10.19.189.22    128.119.245.12   TCP      54 58110 → 80 [ACK] Seq=153076 Ack=778 Win=64512 Len=0                                    6.294464000
 8921 7   10.19.189.22    13.107.137.11    TCP      54 50111 → 443 [ACK] Seq=8403990 Ack=2166 Win=255 Len=0                                   7.725602000
 8923 7   10.19.189.22    13.107.137.11    TCP      66 [TCP Dup ACK 8921#1] 50111 → 443 [ACK] Seq=8403990 Ack=2166 Win=255 Len=0 SLE=9…       7.728437000
 8932 8   10.19.189.22    20.189.173.26    TCP      54 53739 → 443 [ACK] Seq=1581 Ack=40 Win=251 Len=0                                        8.072437000
17056 10  10.19.189.22    13.107.137.11    TCP      54 50110 → 443 [ACK] Seq=8403990 Ack=4340 Win=255 Len=0                                  10.079946000
17061 10  10.19.189.22    20.189.173.26    TCP      54 53739 → 443 [ACK] Seq=2496 Ack=233 Win=251 Len=0                                      10.643766000
```

```
Frame 97: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Devi
Ethernet II, Src: AzureWaveTec_5e:ee:a6 (c0:bf:be:5e:ee:a6), Dst: All-HSRP-routers_47
Internet Protocol Version 4, Src: 10.19.189.22, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58110, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
[Community ID: 1:ponZVpPBk+6t1uIykOrNLtE5n9E=]
```

```
0000  00 00 0c 07 ac 47 c0 bf  be 5e ee a6 08 00 45 00   ·····G·· ·^····E·
0010  00 28 5d 56 40 00 80 06  60 cc 0a 13 bd 16 80 77   ·(]V@··· `······w
0020  f5 0c e2 fe 00 50 a6 04  26 36 64 c5 57 ed 50 10   ·····P·· &6d·W·P·
0030  00 ff 05 ec 00 00                                  ······
```

Transmission Control Protocol (tcp), 20 byte(s)　　分组: 24931 · Displayed: 27 (0.1%)　　配置: Default

Figure ACK


tcp_upload.pcapng
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(T) 帮助(H)

```
tcp.stream eq 12
```

```
No.     Time  Source          Destination      Protocol Length Info                                                                      Time (Relative)
  343 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=144327 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985627000
  344 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=145577 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985627000
  345 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=146827 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985627000
  346 5   10.19.189.22    128.119.245.12   TCP     188 58110 → 80 [PSH, ACK] Seq=148077 Ack=1 Win=65280 Len=134 [TCP PDU reassembled i…   5.985627000
  347 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=148211 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985829000
  348 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=149461 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985829000
  349 5   10.19.189.22    128.119.245.12   TCP    1304 58110 → 80 [ACK] Seq=150711 Ack=1 Win=65280 Len=1250 [TCP PDU reassembled in 35…   5.985829000
  350 5   10.19.189.22    128.119.245.12   HTTP   1169 POST /wireshark-labs/lab3-1-reply.htm HTTP/1.1  (text/plain)                      5.985829000
 6614 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=83255 Win=181632 Len=0                                  6.239653000
 6615 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=85755 Win=179584 Len=0                                  6.239653000
 6616 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=92005 Win=195712 Len=0                                  6.239653000
 6617 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=98255 Win=208256 Len=0                                  6.239653000
 6618 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=99505 Win=211200 Len=0                                  6.239653000
 6619 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=103255 Win=218624 Len=0                                 6.239653000
 6620 6   128.119.245.12  10.19.189.22     TCP      54 80 → 58110 [ACK] Seq=1 Ack=109505 Win=227840 Len=0                                 6.239653000
```

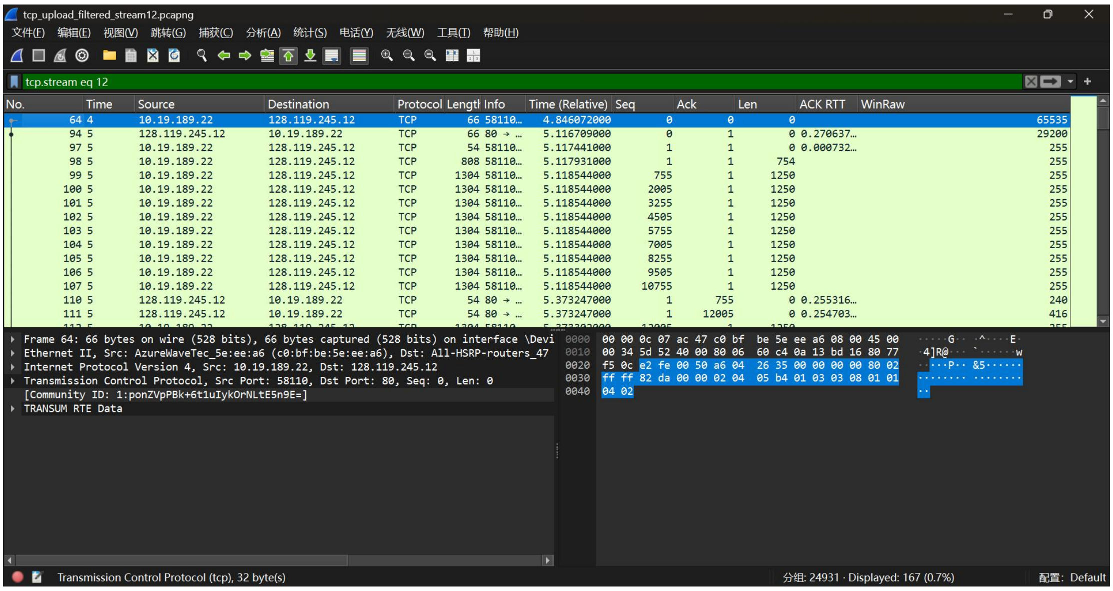
```
Frame 350: 1169 bytes on wire (9352 bits), 1169 bytes captured (9352 bits) on interfac
Ethernet II, Src: AzureWaveTec_5e:ee:a6 (c0:bf:be:5e:ee:a6), Dst: All-HSRP-routers_47
Internet Protocol Version 4, Src: 10.19.189.22, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58110, Dst Port: 80, Seq: 151961, Ack: 1, Len
[[…] 125 Reassembled TCP Segments (153075 bytes): #98(754), #99(1250), #100(1250), #10
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----WebKitFo
[Community ID: 1:ponZVpPBk+6t1uIykOrNLtE5n9E=]
TRANSUM RTE Data
```

```
0020  f5 0c e2 fe 00 50 a6 06  77 ce 64 c5 57 ed 50 18   ·····P·· w·d·W·P·
0030  00 ff d9 bc 00 00 73 74  6c 69 6e 67 20 69 6e 20   ······st ling in 
0040  74 68 65 20 77 69 6e 64  2c 20 61 6e 64 20 74 68   the wind , and th
0050  65 20 70 6f 6f 6c 20 72  69 70 70 6c 69 6e 67 20   e pool r ippling 
0060  74 6f 20 74 68 65 20 77  61 76 69 6e 67 20 6f 66   to the w aving of
0070  20 74 68 65 0d 0a 72 65  65 64 73 2d 2d 74 68 65    the··re eds--the
0080  20 72 61 74 74 6c 69 6e  67 20 74 65 61 63 75 70    rattlin g teacup
0090  73 20 77 6f 75 6c 64 20  63 68 61 6e 67 65 20 74   s would  change t
00a0  6f 20 74 69 6e 6b 6c 69  6e 67 20 73 68 65 65 70   o tinkli ng sheep
00b0  2d 0d 0a 62 65 6c 6c 73  2c 20 61 6e 64 20 74 68   -··bells , and th
00c0  65 20 51 75 65 65 6e 27  73 20 73 68 72 69 6c 6c   e Queen' s shrill
00d0  20 63 72 69 65 73 20 74  6f 20 74 68 65 20 76 6f    cries t o the vo
00e0  69 63 65 20 6f 66 20 74  68 65 20 73 68 65 70 68   ice of t he sheph
00f0  65 72 64 0d 0a 62 6f 79  2d 2d 61 6e 64 20 74 68   erd··boy --and th
0100  65 20 73 6e 65 65 7a 65  20 6f 66 20 74 68 65 20   e sneeze  of the 
0110  62 61 62 79 2c 20 74 68  65 20 73 68 72 69 65 6b   baby, th e shriek
```

Frame (1169 bytes)　Reassembled TCP (153075 bytes)

Transmission Control Protocol (tcp), 20 byte(s)　　分组: 24931 · Displayed: 167 (0.7%)　　配置: Default

Figure http post



tcp.stream eq 12

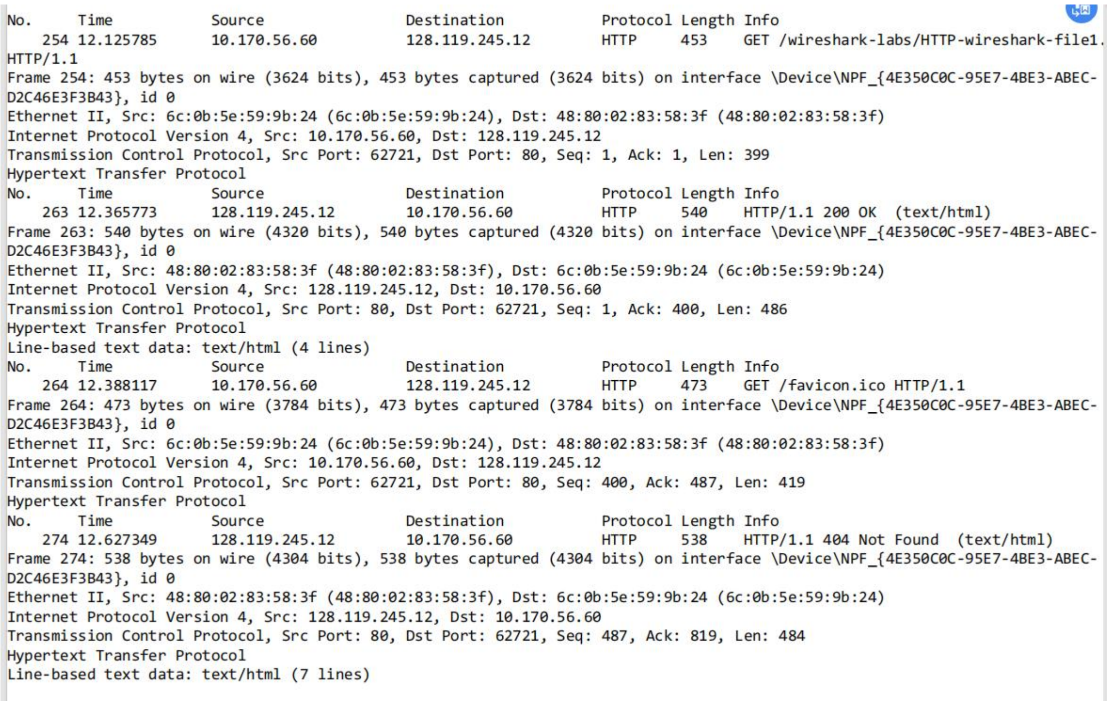
No.	Time	Source	Destination	Protocol	Length	Info	Time (Relative)	Seq	Ack	Len	ACK RTT	WinRaw
64	4	10.19.189.22	128.119.245.12	TCP	66	58110…	4.846072000	0	0	0		65535
94	5	128.119.245.12	10.19.189.22	TCP	66	80 → …	5.116709000	0	1	0	0.270637…	29200
97	5	10.19.189.22	128.119.245.12	TCP	54	58110…	5.117441000	1	1	0	0.000732…	255
98	5	10.19.189.22	128.119.245.12	TCP	808	58110…	5.117931000	1	1	754		255
99	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	755	1	1250		255
100	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	2005	1	1250		255
101	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	3255	1	1250		255
102	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	4505	1	1250		255
103	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	5755	1	1250		255
104	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	7005	1	1250		255
105	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	8255	1	1250		255
106	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	9505	1	1250		255
107	5	10.19.189.22	128.119.245.12	TCP	1304	58110…	5.118544000	10755	1	1250		255
110	5	128.119.245.12	10.19.189.22	TCP	54	80 → …	5.373247000	1	755	0	0.255316…	240
111	5	128.119.245.12	10.19.189.22	TCP	54	80 → …	5.373247000	1	12005	0	0.254703…	416

```
Frame 64: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Devi
Ethernet II, Src: AzureWaveTec_5e:ee:a6 (c0:bf:be:5e:ee:a6), Dst: All-HSRP-routers_47
Internet Protocol Version 4, Src: 10.19.189.22, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 58110, Dst Port: 80, Seq: 0, Len: 0
[Community ID: 1:ponZVpPBk+6t1uIykOrNLtE5n9E=]
TRANSUM RTE Data
```

```
0000  00 00 0c 07 ac 47 c0 bf  be 5e ee a6 08 00 45 00   ·····G·· ·^····E·
0010  00 34 5d 52 40 00 80 06  60 c4 0a 13 bd 16 80 77   ·4]R@··· `······w
0020  f5 0c e2 fe 00 50 a6 04  26 35 00 00 00 00 80 02   ·····P·· &5······
0030  ff ff 82 da 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

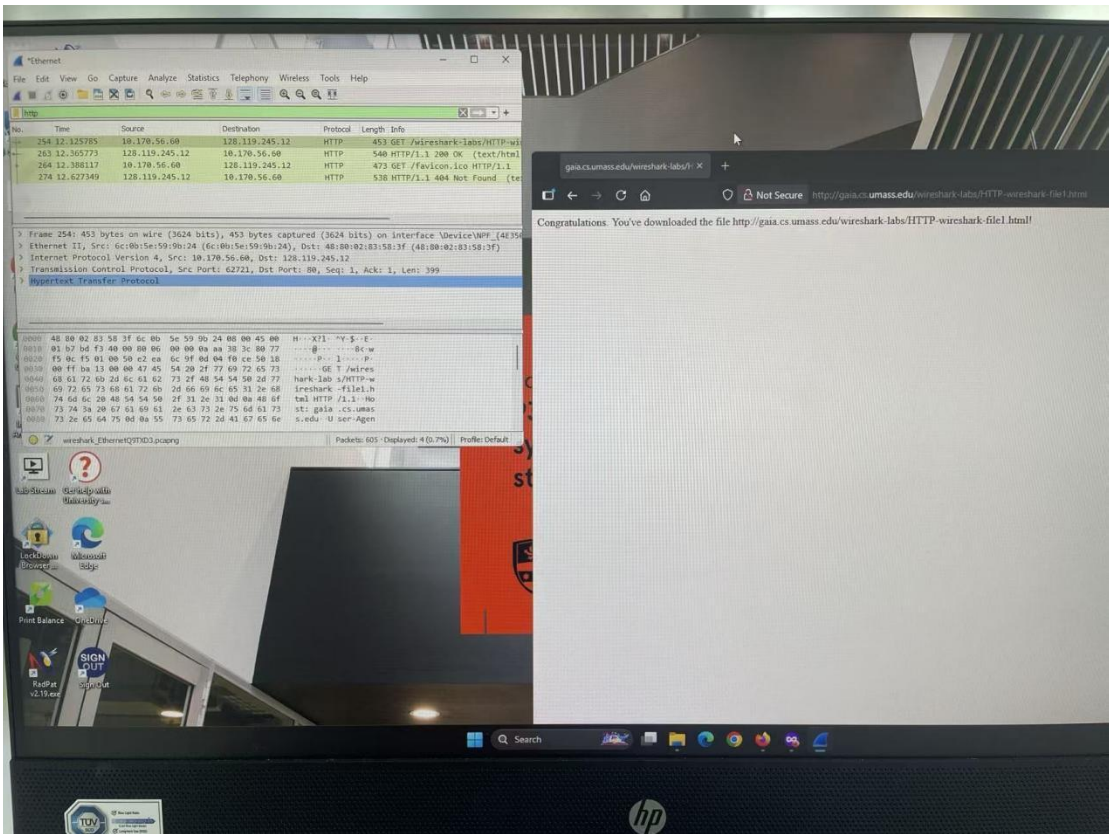
Transmission Control Protocol (tcp), 32 byte(s)   分组: 24931 · Displayed: 167 (0.7%)   配置: Default

Figure RTT and Estimated RTT



```
No.     Time           Source                Destination           Protocol Length Info
    254 12.125785      10.170.56.60          128.119.245.12        HTTP     453    GET /wireshark-labs/HTTP-wireshark-file1.
HTTP/1.1
Frame 254: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62721, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    263 12.365773      128.119.245.12        10.170.56.60          HTTP     540    HTTP/1.1 200 OK  (text/html)
Frame 263: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 62721, Seq: 1, Ack: 400, Len: 486
Hypertext Transfer Protocol
Line-based text data: text/html (4 lines)
No.     Time           Source                Destination           Protocol Length Info
    264 12.388117      10.170.56.60          128.119.245.12        HTTP     473    GET /favicon.ico HTTP/1.1
Frame 264: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 62721, Dst Port: 80, Seq: 400, Ack: 487, Len: 419
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    274 12.627349      128.119.245.12        10.170.56.60          HTTP     538    HTTP/1.1 404 Not Found  (text/html)
Frame 274: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 62721, Seq: 487, Ack: 819, Len: 484
Hypertext Transfer Protocol
Line-based text data: text/html (7 lines)
```

2.1 printed file

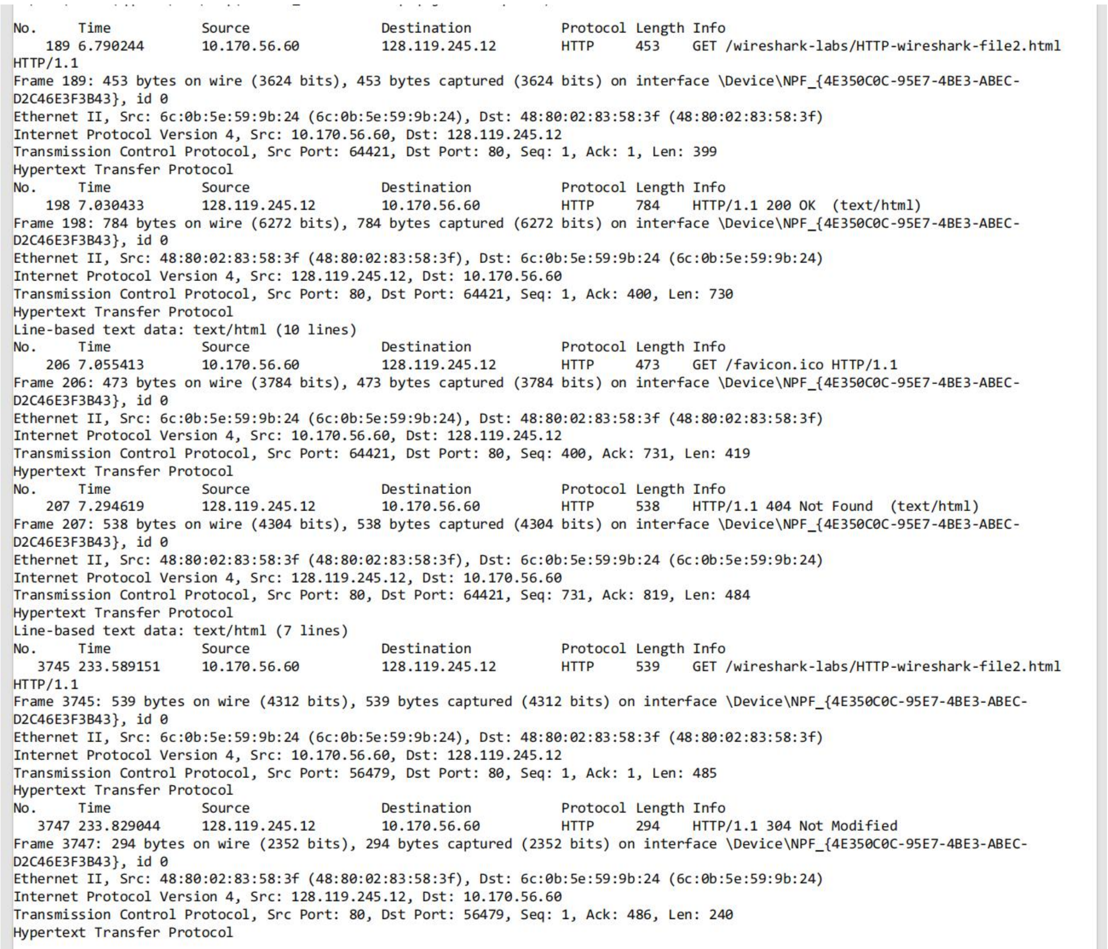


```
No.   Time        Source          Destination     Protocol Length Info
  254 12.125785   10.170.56.60    128.119.245.12  HTTP     453 GET /wireshark-labs/HTTP-wi
  263 12.365773   128.119.245.12  10.170.56.60    HTTP     540 HTTP/1.1 200 OK  (text/html
  264 12.388117   10.170.56.60    128.119.245.12  HTTP     473 GET /favicon.ico HTTP/1.1
  274 12.627349   128.119.245.12  10.170.56.60    HTTP     538 HTTP/1.1 404 Not Found  (te

> Frame 254: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E35
> Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
> Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 62721, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
> Hypertext Transfer Protocol

0000  48 80 02 83 58 3f 6c 0b  5e 59 9b 24 08 00 45 00   H···X?l· ^Y·$··E·
0010  01 b7 bd f3 40 00 80 06  00 00 0a aa 38 3c 80 77   ····@··· ····8<·w
0020  f5 0c f5 01 00 50 c2 ea  6c 9f 0d 04 f0 ce 50 18   ·····P·· l·····P·
0030  00 ff ba 13 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 31 2e 68   ireshark -file1.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen

wireshark_EthernetQ9TXD3.pcapng    Packets: 605 · Displayed: 4 (0.7%)    Profile: Default
```

Congratulations. You've downloaded the file http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html!

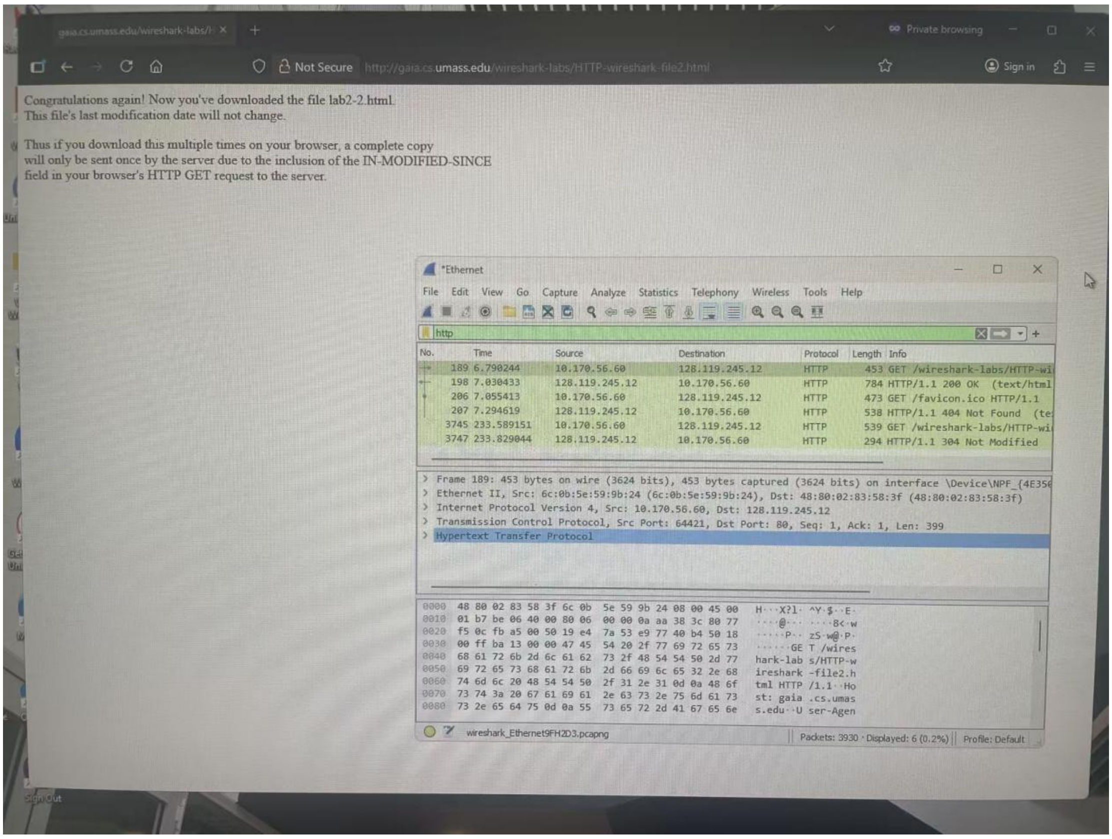
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
gaia.cs.umass.edu/wireshark-labs/H
Not Secure
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
Lab Stream
Get help with University ...
LockDown Browser ...
Microsoft Edge
Print Balance
OneDrive
RadPat v2.19.exe
SIGN OUT
Sign Out
Search

2.1 set up



```
No.     Time           Source                Destination           Protocol Length Info
    189 6.790244       10.170.56.60          128.119.245.12        HTTP     453    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 189: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64421, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    198 7.030433       128.119.245.12        10.170.56.60          HTTP     784    HTTP/1.1 200 OK  (text/html)
Frame 198: 784 bytes on wire (6272 bits), 784 bytes captured (6272 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 64421, Seq: 1, Ack: 400, Len: 730
Hypertext Transfer Protocol
Line-based text data: text/html (10 lines)
No.     Time           Source                Destination           Protocol Length Info
    206 7.055413       10.170.56.60          128.119.245.12        HTTP     473    GET /favicon.ico HTTP/1.1
Frame 206: 473 bytes on wire (3784 bits), 473 bytes captured (3784 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 64421, Dst Port: 80, Seq: 400, Ack: 731, Len: 419
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    207 7.294619       128.119.245.12        10.170.56.60          HTTP     538    HTTP/1.1 404 Not Found  (text/html)
Frame 207: 538 bytes on wire (4304 bits), 538 bytes captured (4304 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 64421, Seq: 731, Ack: 819, Len: 484
Hypertext Transfer Protocol
Line-based text data: text/html (7 lines)
No.     Time           Source                Destination           Protocol Length Info
   3745 233.589151     10.170.56.60          128.119.245.12        HTTP     539    GET /wireshark-labs/HTTP-wireshark-file2.html
HTTP/1.1
Frame 3745: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 56479, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
   3747 233.829044     128.119.245.12        10.170.56.60          HTTP     294    HTTP/1.1 304 Not Modified
Frame 3747: 294 bytes on wire (2352 bits), 294 bytes captured (2352 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 56479, Seq: 1, Ack: 486, Len: 240
Hypertext Transfer Protocol
```

2.2 printed file


gaia.cs.umass.edu/wireshark-labs/H
Private browsing
Not Secure
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html
Sign in

Congratulations again! Now you've downloaded the file lab2-2.html.
This file's last modification date will not change.

Thus if you download this multiple times on your browser, a complete copy
will only be sent once by the server due to the inclusion of the IN-MODIFIED-SINCE
field in your browser's HTTP GET request to the server.

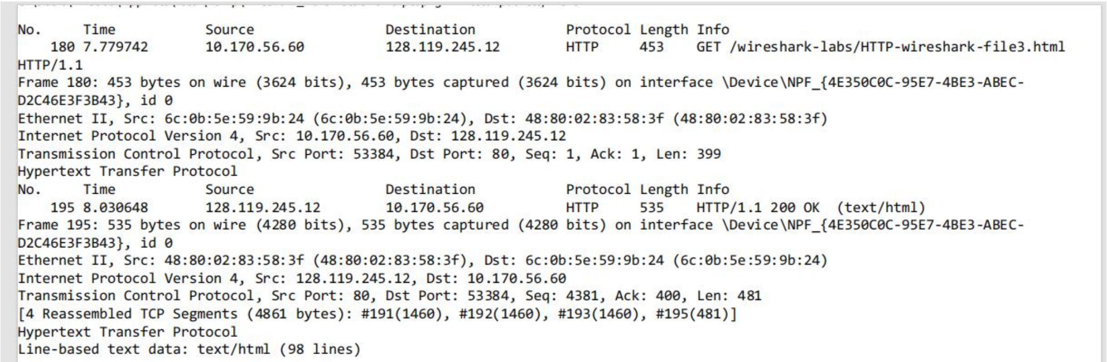
*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

```
No.    Time         Source          Destination     Protocol  Length Info
  189 6.790244      10.170.56.60    128.119.245.12  HTTP        453 GET /wireshark-labs/HTTP-wi
  198 7.030433      128.119.245.12  10.170.56.60    HTTP        784 HTTP/1.1 200 OK  (text/html
  206 7.055413      10.170.56.60    128.119.245.12  HTTP        473 GET /favicon.ico HTTP/1.1
  207 7.294619      128.119.245.12  10.170.56.60    HTTP        538 HTTP/1.1 404 Not Found  (te
 3745 233.589151    10.170.56.60    128.119.245.12  HTTP        539 GET /wireshark-labs/HTTP-wi
 3747 233.829044    128.119.245.12  10.170.56.60    HTTP        294 HTTP/1.1 304 Not Modified

> Frame 189: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E35
> Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
> Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 64421, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
> Hypertext Transfer Protocol

0000  48 80 02 83 58 3f 6c 0b  5e 59 9b 24 08 00 45 00   H···X?l· ^Y·$··E·
0010  01 b7 be 06 40 00 80 06  00 00 0a aa 38 3c 80 77   ····@··· ····8<·w
0020  f5 0c fb a5 00 50 19 e4  7a 53 e9 77 40 b4 50 18   ·····P·· zS·w@·P·
0030  00 ff ba 13 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 32 2e 68   ireshark -file2.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
```

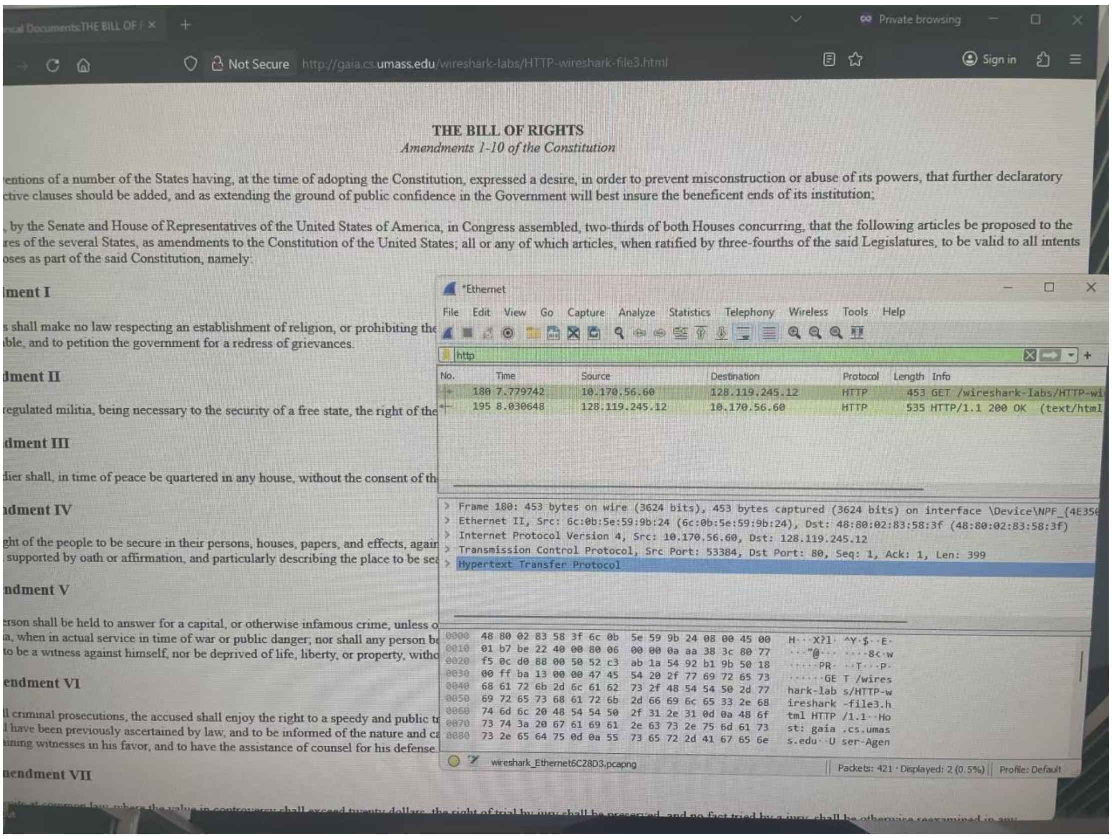
wireshark_Ethernet9FH2D3.pcapng | Packets: 3930 · Displayed: 6 (0.2%) | Profile: Default

2.2 set up



```
No.     Time           Source                Destination           Protocol Length Info
    180 7.779742       10.170.56.60          128.119.245.12        HTTP     453    GET /wireshark-labs/HTTP-wireshark-file3.html 
HTTP/1.1 
Frame 180: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 53384, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    195 8.030648       128.119.245.12        10.170.56.60          HTTP     535    HTTP/1.1 200 OK  (text/html)
Frame 195: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 53384, Seq: 4381, Ack: 400, Len: 481
[4 Reassembled TCP Segments (4861 bytes): #191(1460), #192(1460), #193(1460), #195(481)]
Hypertext Transfer Protocol
Line-based text data: text/html (98 lines)
```

2.3 printed file



ical Documents:THE BILL OF F
Private browsing
Not Secure
http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html
Sign in

THE BILL OF RIGHTS
Amendments 1-10 of the Constitution

entions of a number of the States having, at the time of adopting the Constitution, expressed a desire, in order to prevent misconstruction or abuse of its powers, that further declaratory ctive clauses should be added, and as extending the ground of public confidence in the Government will best insure the beneficent ends of its institution;

, by the Senate and House of Representatives of the United States of America, in Congress assembled, two-thirds of both Houses concurring, that the following articles be proposed to the res of the several States, as amendments to the Constitution of the United States; all or any of which articles, when ratified by three-fourths of the said Legislatures, to be valid to all intents oses as part of the said Constitution, namely:

lment I

s shall make no law respecting an establishment of religion, or prohibiting the
ble, and to petition the government for a redress of grievances.

dment II

regulated militia, being necessary to the security of a free state, the right of the

dment III

dier shall, in time of peace be quartered in any house, without the consent of th

ndment IV

ght of the people to be secure in their persons, houses, papers, and effects, again
supported by oath or affirmation, and particularly describing the place to be sea

ndment V

rson shall be held to answer for a capital, or otherwise infamous crime, unless o
a, when in actual service in time of war or public danger; nor shall any person be
to be a witness against himself, nor be deprived of life, liberty, or property, witho

endment VI

l criminal prosecutions, the accused shall enjoy the right to a speedy and public tr
l have been previously ascertained by law, and to be informed of the nature and ca
ining witnesses in his favor, and to have the assistance of counsel for his defense.

nendment VII

*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

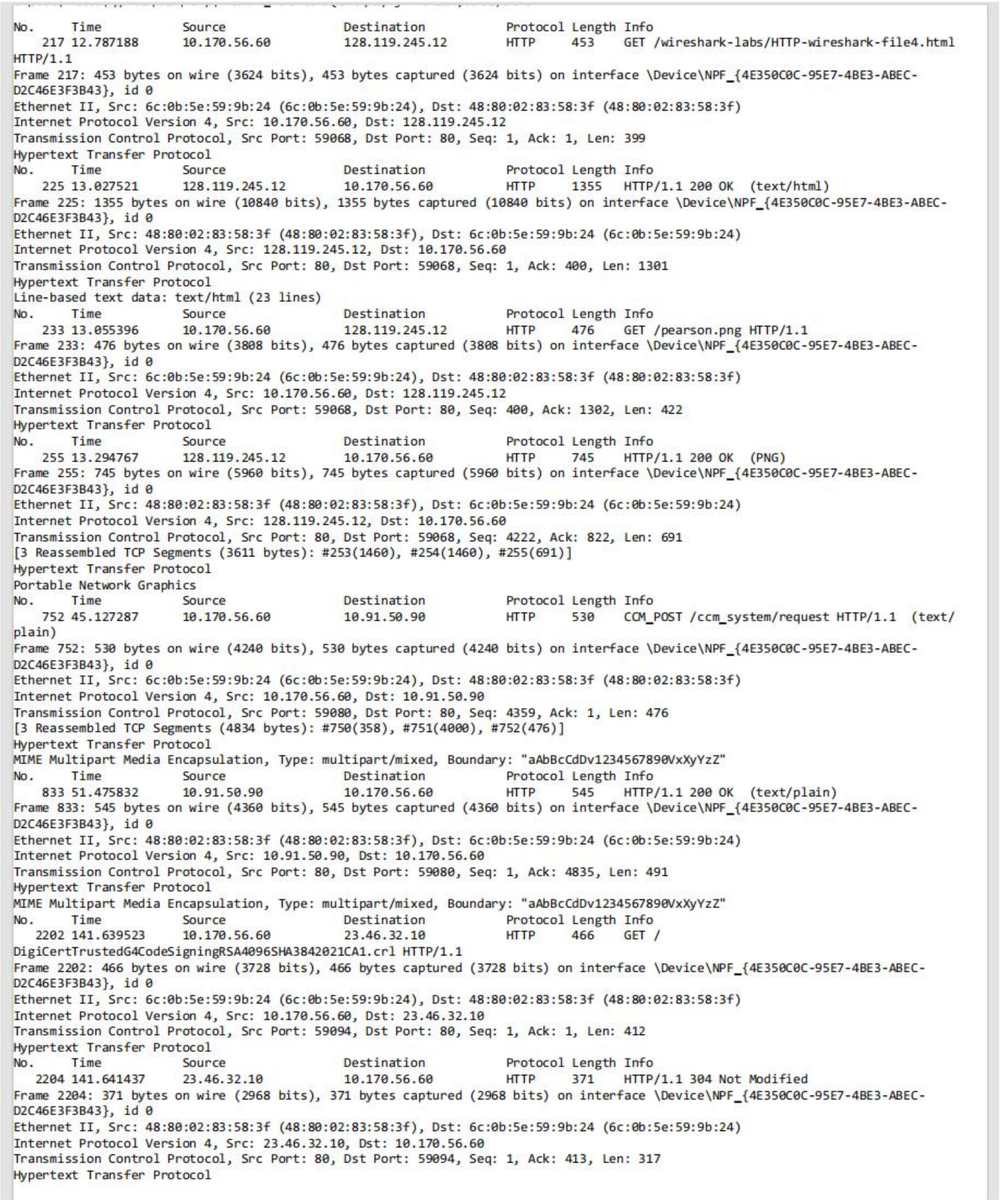
No.	Time	Source	Destination	Protocol	Length	Info
180	7.779742	10.170.56.60	128.119.245.12	HTTP	453	GET /wireshark-labs/HTTP-wi
195	8.030648	128.119.245.12	10.170.56.60	HTTP	535	HTTP/1.1 200 OK (text/html

```
> Frame 180: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E35
> Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
> Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 53384, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
> Hypertext Transfer Protocol
```

```
0000  48 80 02 83 58 3f 6c 0b  5e 59 9b 24 08 00 45 00   H···X?l· ^Y·$··E·
0010  01 b7 be 22 40 00 80 06  00 00 0a aa 38 3c 80 77   ···"@··· ····8<·w
0020  f5 0c d0 88 00 50 52 c3  ab 1a 54 92 b1 9b 50 18   ·····PR· ··T···P·
0030  00 ff ba 13 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 33 2e 68   ireshark -file3.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
```

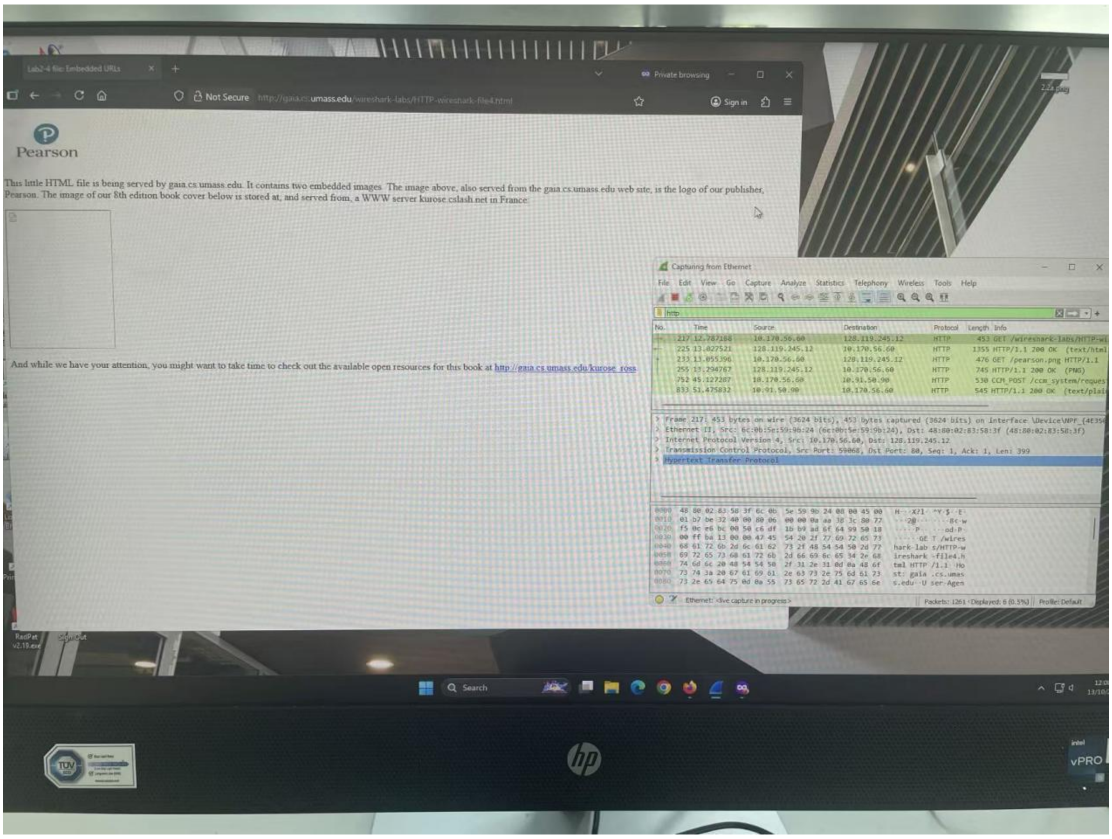
wireshark_Ethernet6CZ8D3.pcapng
Packets: 421 · Displayed: 2 (0.5%)
Profile: Default

2.3 set up



```
No.     Time           Source                Destination           Protocol Length Info
    217 12.787188      10.170.56.60          128.119.245.12        HTTP     453    GET /wireshark-labs/HTTP-wireshark-file4.html
HTTP/1.1
Frame 217: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59068, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    225 13.027521      128.119.245.12        10.170.56.60          HTTP     1355   HTTP/1.1 200 OK  (text/html)
Frame 225: 1355 bytes on wire (10840 bits), 1355 bytes captured (10840 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 59068, Seq: 1, Ack: 400, Len: 1301
Hypertext Transfer Protocol
Line-based text data: text/html (23 lines)
No.     Time           Source                Destination           Protocol Length Info
    233 13.055396      10.170.56.60          128.119.245.12        HTTP     476    GET /pearson.png HTTP/1.1
Frame 233: 476 bytes on wire (3808 bits), 476 bytes captured (3808 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 59068, Dst Port: 80, Seq: 400, Ack: 1302, Len: 422
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    255 13.294767      128.119.245.12        10.170.56.60          HTTP     745    HTTP/1.1 200 OK  (PNG)
Frame 255: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 59068, Seq: 4222, Ack: 822, Len: 691
[3 Reassembled TCP Segments (3611 bytes): #253(1460), #254(1460), #255(691)]
Hypertext Transfer Protocol
Portable Network Graphics
No.     Time           Source                Destination           Protocol Length Info
    752 45.127287      10.170.56.60          10.91.50.90           HTTP     530    CCM_POST /ccm_system/request HTTP/1.1  (text/
plain)
Frame 752: 530 bytes on wire (4240 bits), 530 bytes captured (4240 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 10.91.50.90
Transmission Control Protocol, Src Port: 59080, Dst Port: 80, Seq: 4359, Ack: 1, Len: 476
[3 Reassembled TCP Segments (4834 bytes): #750(358), #751(4000), #752(476)]
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "aAbBcCdDv1234567890VxXyYzZ"
No.     Time           Source                Destination           Protocol Length Info
    833 51.475832      10.91.50.90           10.170.56.60          HTTP     545    HTTP/1.1 200 OK  (text/plain)
Frame 833: 545 bytes on wire (4360 bits), 545 bytes captured (4360 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 10.91.50.90, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 59080, Seq: 1, Ack: 4835, Len: 491
Hypertext Transfer Protocol
MIME Multipart Media Encapsulation, Type: multipart/mixed, Boundary: "aAbBcCdDv1234567890VxXyYzZ"
No.     Time           Source                Destination           Protocol Length Info
   2202 141.639523     10.170.56.60          23.46.32.10           HTTP     466    GET /
DigiCertTrustedG4CodeSigningRSA4096SHA3842021CA1.crl HTTP/1.1
Frame 2202: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 23.46.32.10
Transmission Control Protocol, Src Port: 59094, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
   2204 141.641437     23.46.32.10           10.170.56.60          HTTP     371    HTTP/1.1 304 Not Modified
Frame 2204: 371 bytes on wire (2968 bits), 371 bytes captured (2968 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 23.46.32.10, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 59094, Seq: 1, Ack: 413, Len: 317
Hypertext Transfer Protocol
```

2.4 printed file



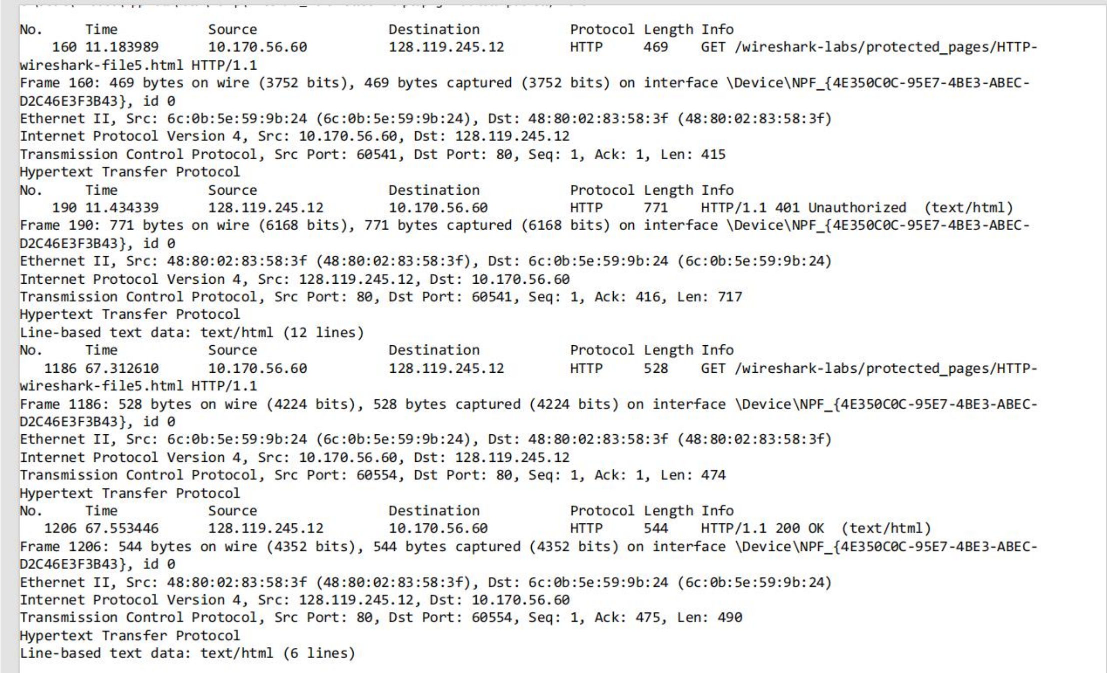
Lab2-4 file: Embedded URLs
Private browsing
Not Secure http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html
Sign in
Pearson
Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

This little HTML file is being served by gaia.cs.umass.edu. It contains two embedded images. The image above, also served from the gaia.cs.umass.edu web site, is the logo of our publisher, Pearson. The image of our 8th edition book cover below is stored at, and served from, a WWW server kurose.cslash.net in France.

And while we have your attention, you might want to take time to check out the available open resources for this book at http://gaia.cs.umass.edu/kurose_ross.

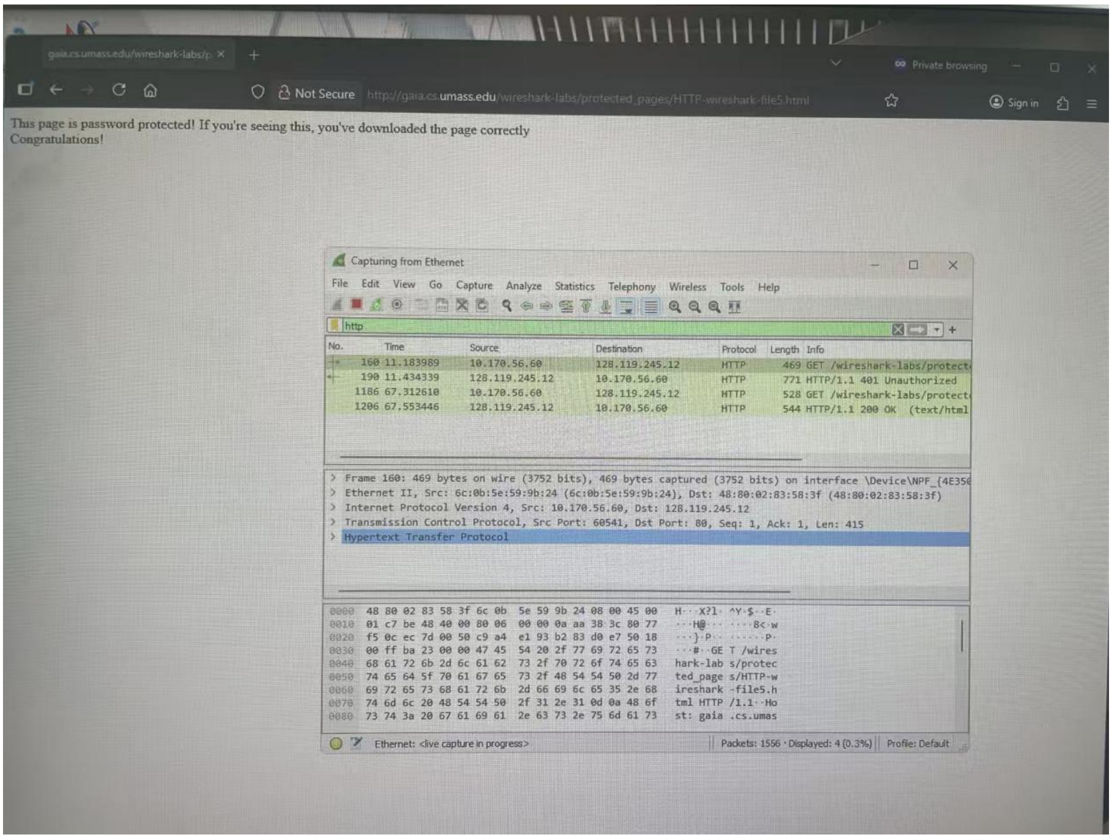
```
No.   Time        Source          Destination     Protocol Length Info
  217 12.787188   10.170.56.60    128.119.245.12  HTTP      453 GET /wireshark-labs/HTTP-wi
  225 13.027521   128.119.245.12  10.170.56.60    HTTP     1355 HTTP/1.1 200 OK  (text/html
  233 13.055396   10.170.56.60    128.119.245.12  HTTP      476 GET /pearson.png HTTP/1.1
  255 13.294767   128.119.245.12  10.170.56.60    HTTP      745 HTTP/1.1 200 OK  (PNG)
  752 45.127287   10.170.56.60    10.91.50.90     HTTP      530 CCM_POST /ccm_system/reques
  833 51.475832   10.91.50.90     10.170.56.60    HTTP      545 HTTP/1.1 200 OK  (text/plai

> Frame 217: 453 bytes on wire (3624 bits), 453 bytes captured (3624 bits) on interface \Device\NPF_{4E35
> Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
> Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 59068, Dst Port: 80, Seq: 1, Ack: 1, Len: 399
> Hypertext Transfer Protocol

0000  48 80 02 83 58 3f 6c 0b  5e 59 9b 24 08 00 45 00   H···X?l· ^Y·$··E·
0010  01 b7 be 32 40 00 80 06  00 00 0a aa 38 3c 80 77   ···2@··· ····8<·w
0020  f5 0c e6 bc 00 50 c6 df  1b b9 ad 6f 64 99 50 18   ·····P·· ···od·P·
0030  00 ff ba 13 00 00 47 45  54 20 2f 77 69 72 65 73   ······GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 77   hark-lab s/HTTP-w
0050  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 34 2e 68   ireshark -file4.h
0060  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0070  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
0080  73 2e 65 64 75 0d 0a 55  73 65 72 2d 41 67 65 6e   s.edu··U ser-Agen
```

2.4 set up



```
No.     Time           Source                Destination           Protocol Length Info
    160 11.183989      10.170.56.60          128.119.245.12        HTTP     469    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 160: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60541, Dst Port: 80, Seq: 1, Ack: 1, Len: 415
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
    190 11.434339      128.119.245.12        10.170.56.60          HTTP     771    HTTP/1.1 401 Unauthorized  (text/html)
Frame 190: 771 bytes on wire (6168 bits), 771 bytes captured (6168 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 60541, Seq: 1, Ack: 416, Len: 717
Hypertext Transfer Protocol
Line-based text data: text/html (12 lines)
No.     Time           Source                Destination           Protocol Length Info
   1186 67.312610      10.170.56.60          128.119.245.12        HTTP     528    GET /wireshark-labs/protected_pages/HTTP-
wireshark-file5.html HTTP/1.1
Frame 1186: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 60554, Dst Port: 80, Seq: 1, Ack: 1, Len: 474
Hypertext Transfer Protocol
No.     Time           Source                Destination           Protocol Length Info
   1206 67.553446      128.119.245.12        10.170.56.60          HTTP     544    HTTP/1.1 200 OK  (text/html)
Frame 1206: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface \Device\NPF_{4E350C0C-95E7-4BE3-ABEC-
D2C46E3F3B43}, id 0
Ethernet II, Src: 48:80:02:83:58:3f (48:80:02:83:58:3f), Dst: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.170.56.60
Transmission Control Protocol, Src Port: 80, Dst Port: 60554, Seq: 1, Ack: 475, Len: 490
Hypertext Transfer Protocol
Line-based text data: text/html (6 lines)
```

2.5 printed file



gaia.cs.umass.edu/wireshark-labs/p
Private browsing
Not Secure
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Sign in

This page is password protected! If you're seeing this, you've downloaded the page correctly
Congratulations!

Capturing from Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
160	11.183989	10.170.56.60	128.119.245.12	HTTP	469	GET /wireshark-labs/protect
190	11.434339	128.119.245.12	10.170.56.60	HTTP	771	HTTP/1.1 401 Unauthorized
1186	67.312610	10.170.56.60	128.119.245.12	HTTP	528	GET /wireshark-labs/protect
1206	67.553446	128.119.245.12	10.170.56.60	HTTP	544	HTTP/1.1 200 OK (text/html

```
> Frame 160: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface \Device\NPF_{4E35
> Ethernet II, Src: 6c:0b:5e:59:9b:24 (6c:0b:5e:59:9b:24), Dst: 48:80:02:83:58:3f (48:80:02:83:58:3f)
> Internet Protocol Version 4, Src: 10.170.56.60, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 60541, Dst Port: 80, Seq: 1, Ack: 1, Len: 415
> Hypertext Transfer Protocol
```

```
0000  48 80 02 83 58 3f 6c 0b  5e 59 9b 24 08 00 45 00   H··X?l· ^Y·$··E·
0010  01 c7 be 48 40 00 80 06  00 00 0a aa 38 3c 80 77   ···H@··· ····8<·w
0020  f5 0c ec 7d 00 50 c9 a4  e1 93 b2 83 d0 e7 50 18   ···}·P·· ······P·
0030  00 ff ba 23 00 00 47 45  54 20 2f 77 69 72 65 73   ···#··GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 70 72 6f 74 65 63   hark-lab s/protec
0050  74 65 64 5f 70 61 67 65  73 2f 48 54 54 50 2d 77   ted_page s/HTTP-w
0060  69 72 65 73 68 61 72 6b  2d 66 69 6c 65 35 2e 68   ireshark -file5.h
0070  74 6d 6c 20 48 54 54 50  2f 31 2e 31 0d 0a 48 6f   tml HTTP /1.1··Ho
0080  73 74 3a 20 67 61 69 61  2e 63 73 2e 75 6d 61 73   st: gaia .cs.umas
```

Ethernet: <live capture in progress>

Packets: 1556 · Displayed: 4 (0.3%)

Profile: Default

2.5 set up