CNT 4704
Analysis of Computer Communication Networks

Introduction to Wireshark

Mesut Ozdag, Ph.D.

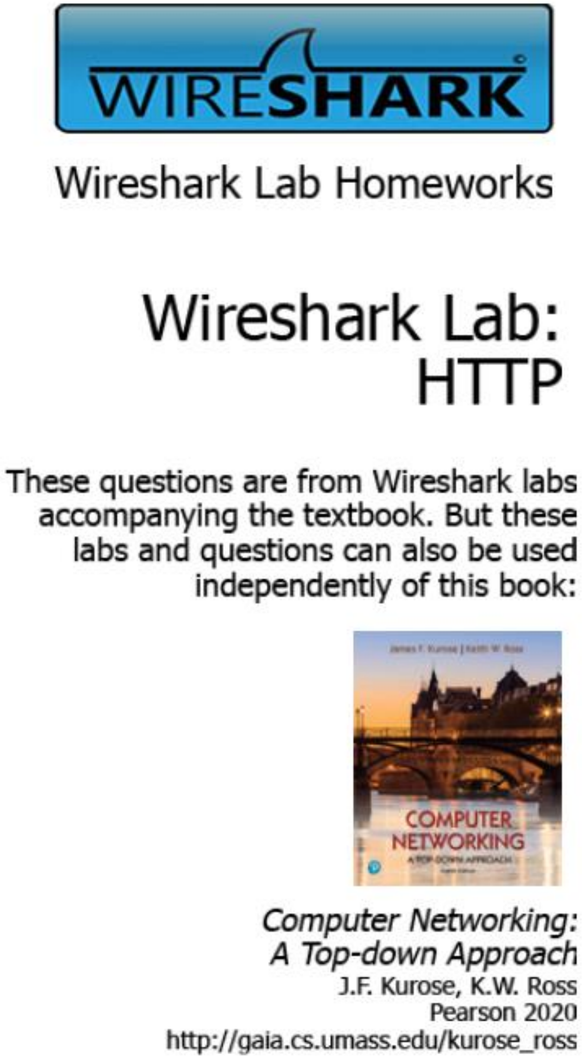
Department of Computer Science

Fall 2024

HOUSEKEEPING & ACKNOWLEDGEMENT

This class session is **being recorded**

- An ample portion of the material is derived/borrowed from Copyrighted ppt. slides of J.F. Kurose, K.W. Ross 1996-2020. All Rights Reserved.
- Original material can be found on: https://gaia.cs.umass.edu/kurose_ross/wireshark.php



Wireshark Lab Homeworks

Wireshark Lab: HTTP

These questions are from Wireshark labs accompanying the textbook. But these labs and questions can also be used independently of this book:

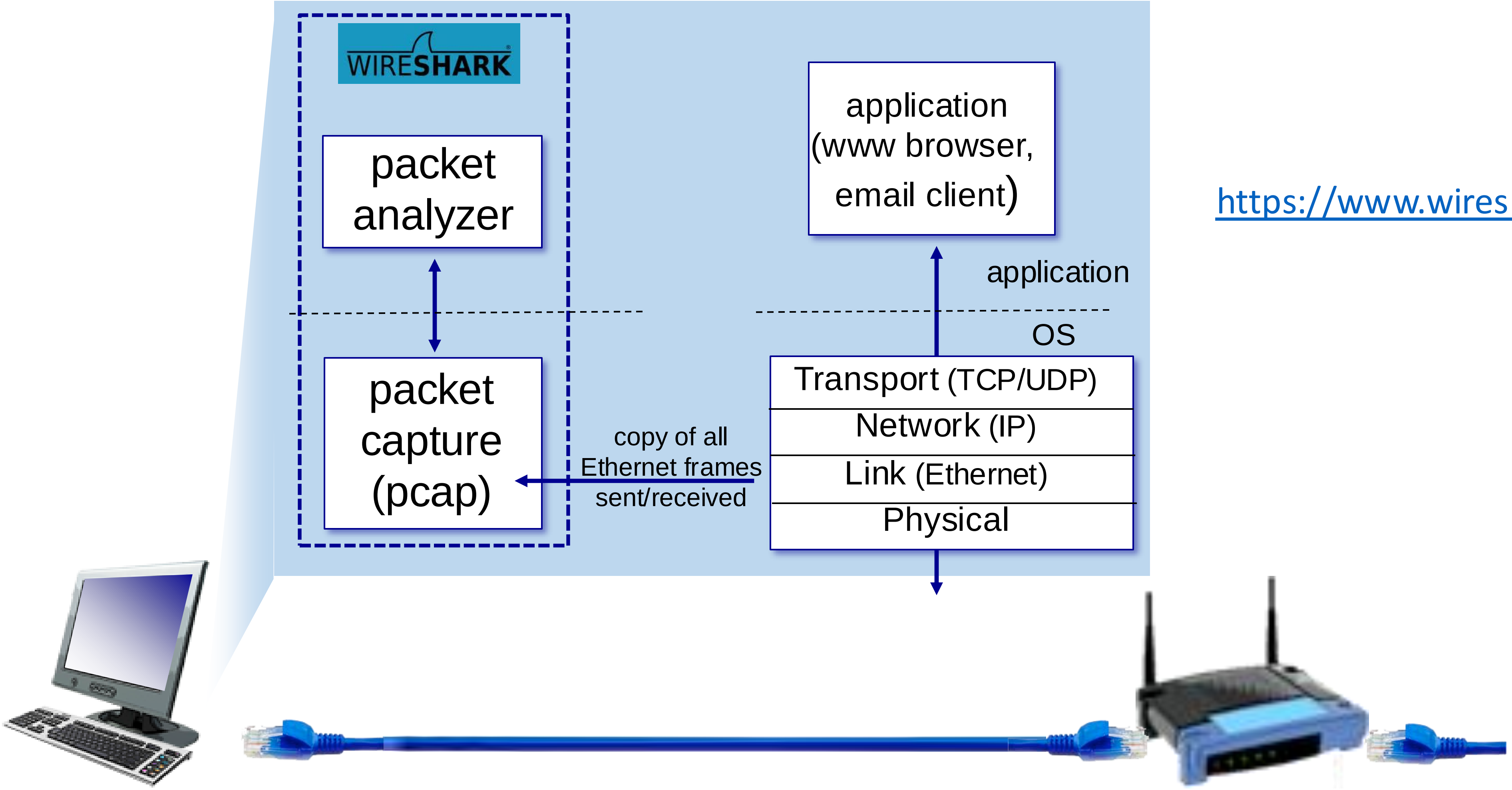
Computer Networking: A Top-down Approach
J.F. Kurose, K.W. Ross
Pearson 2020
http://gaia.cs.umass.edu/kurose_ross

WIRESHARK INTRODUCTION LAB

What to expect:

- What is Wireshark?
- How does it work?
- Demonstration
- Understand what you’re seeing
- See how packets are transmitted and get a visual understanding
- Implementing and introducing various functions
  - Filters
  - Menus

Wireshark



https://www.wireshark.org/

Wireshark

- Start up your web browser.

Wireshark

- Start up the Wireshark packet sniffer(but don’t yet begin packet capture). In this example we’re only interested in the HTTP protocol here

Wireshark

- Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.

Wireshark

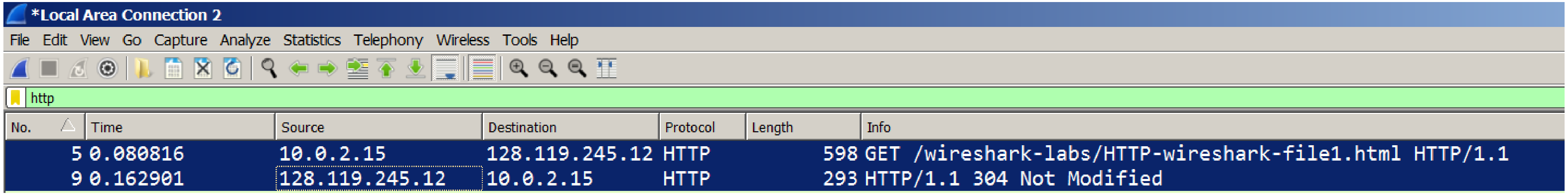
- Enter the following to your browser
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html
  Your browser should display the very simple, one-line HTML file.

Wireshark

- Stop Wireshark packet capture.

Wireshark

- Apply filter http (text only no quotation marks)



http

No.	Time	Source	Destination	Protocol	Length	Info
5	0.080816	10.0.2.15	128.119.245.12	HTTP	598	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
9	0.162901	128.119.245.12	10.0.2.15	HTTP	293	HTTP/1.1 304 Not Modified

Wireshark

- GET message (from your browser to the gaia.cs.umass.edu web server)
- Response message from the server to your browser

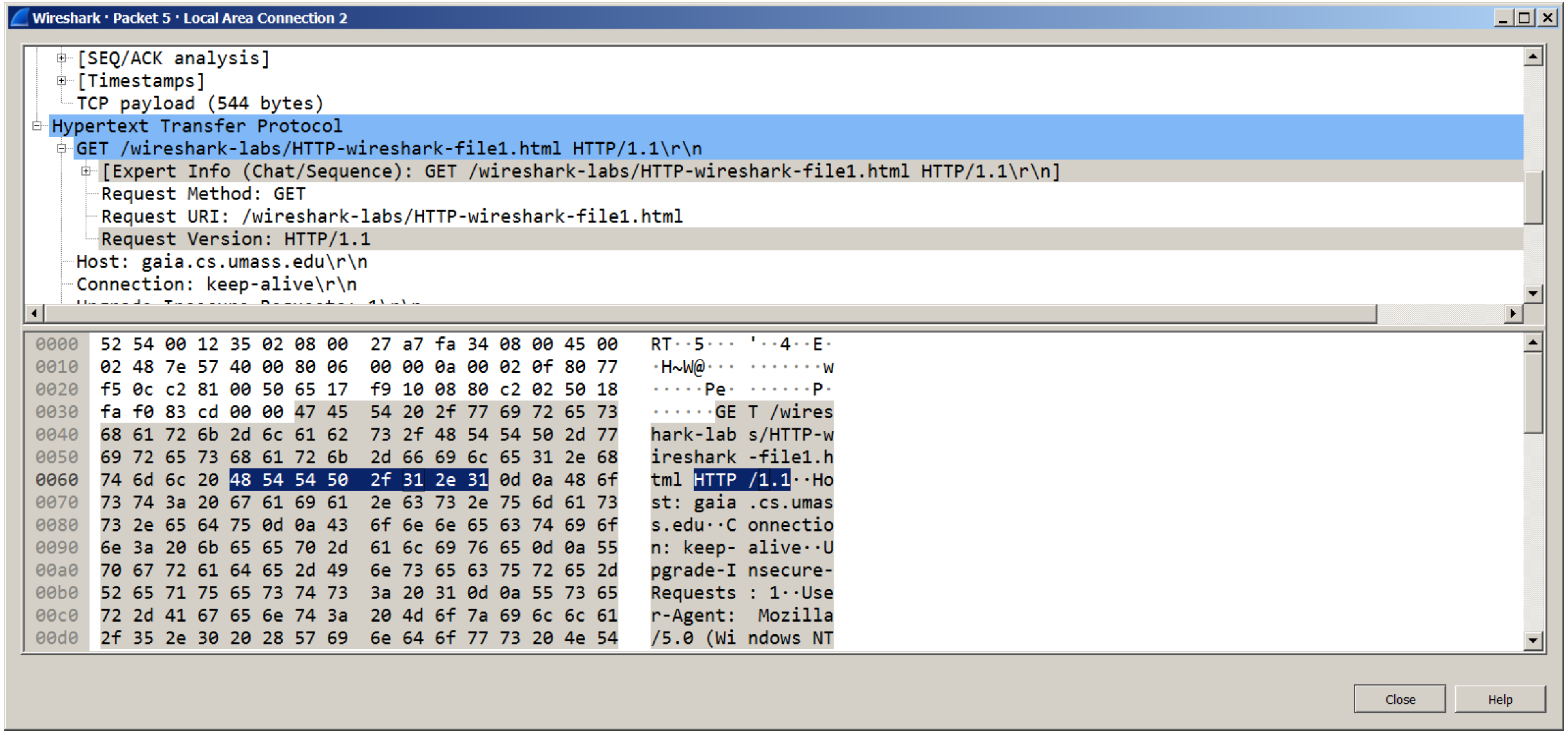
Wireshark

__________________HTTP message was carried inside a
_____________TCP segment, which was carried inside an
_______IP datagram, which was carried within an
Ethernet frame,

- Wireshark displays the Frame, Ethernet, IP, and TCP packet information as well. We want to minimize the amount of **non-HTTP** data displayed

Our example is for HTTP protocol

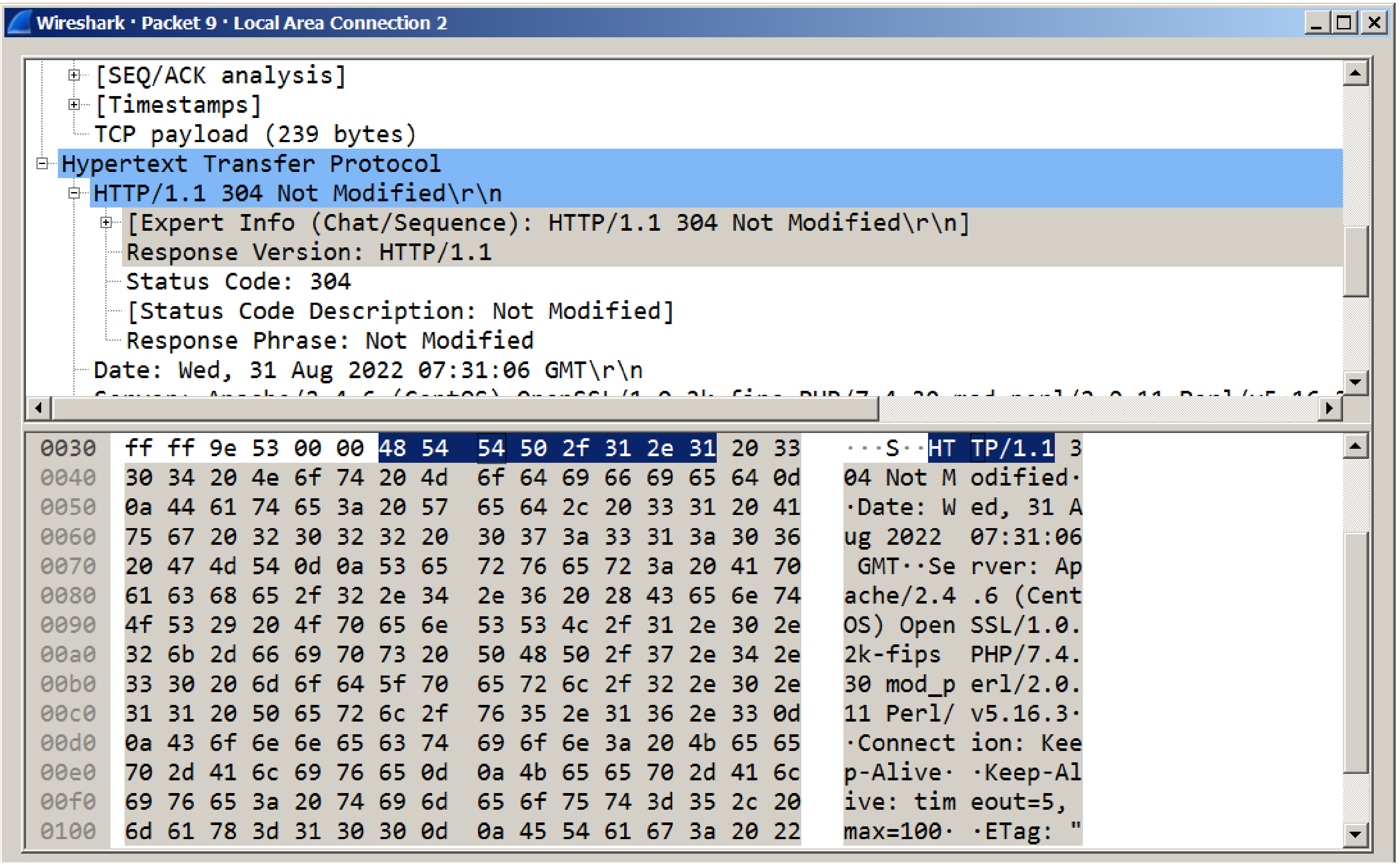
Wireshark



```
    ⊞ [SEQ/ACK analysis]
    ⊞ [Timestamps]
      TCP payload (544 bytes)
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n
    ⊞ [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-wireshark-file1.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
```

```
0000  52 54 00 12 35 02 08 00  27 a7 fa 34 08 00 45 00   RT··5··· '··4··E·
0010  02 48 7e 57 40 00 80 06  00 00 0a 00 02 0f 80 77   ·H~W@··· ·······w
0020  f5 0c c2 81 00 50 65 17  f9 10 08 80 c2 02 50 18   ·····Pe· ······P·
0030  fa f0 83 cd 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 43  6f 6e 6e 65 63 74 69 6f   s.edu··C onnectio
0090  6e 3a 20 6b 65 65 70 2d  61 6c 69 76 65 0d 0a 55   n: keep- alive··U
00a0  70 67 72 61 64 65 2d 49  6e 73 65 63 75 72 65 2d   pgrade-I nsecure-
00b0  52 65 71 75 65 73 74 73  3a 20 31 0d 0a 55 73 65   Requests : 1··Use
00c0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00d0  2f 35 2e 30 20 28 57 69  6e 64 6f 77 73 20 4e 54   /5.0 (Wi ndows NT
```

Wireshark



```
    [SEQ/ACK analysis]
    [Timestamps]
    TCP payload (239 bytes)
Hypertext Transfer Protocol
  HTTP/1.1 304 Not Modified\r\n
    [Expert Info (Chat/Sequence): 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, 31 Aug 2022 07:31:06 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4.30 mod_perl/2.0.11 Perl/v5.16.
```

```
0030  ff ff 9e 53 00 00 48 54  54 50 2f 31 2e 31 20 33   ···S··HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified·
0050  0a 44 61 74 65 3a 20 57  65 64 2c 20 33 31 20 41   ·Date: W ed, 31 A
0060  75 67 20 32 30 32 32 20  30 37 3a 33 31 3a 30 36   ug 2022  07:31:06
0070  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0080  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0090  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
00a0  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
00b0  33 30 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   30 mod_p erl/2.0.
00c0  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
00d0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
00e0  70 2d 41 6c 69 76 65 0d  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 3d 35 2c 20   ive: tim eout=5,
0100  6d 61 78 3d 31 30 30 0d  0a 45 54 61 67 3a 20 22   max=100· ·ETag: "
```

Wireshark

Is your browser running HTTP version 1.0 or 1.1? What version of HTTP is the server running?

Both are HTTP/1.1

Wireshark

What languages (if any) does your browser indicate that it can accept to the server?

Accept-Language: en-US,en;q=0.5\r\n

Wireshark introduction ..

- Check the view drop-down for interface personalization
- Time, source, IP or MAC, Protocol, Info (can be the most important depending on your application)
- Filters:
  - It turns green on valid filters upon writing
  - Looking for a certain protocol packets, i.e. tcp, http
  - It can be case sensitive in some commands that required text

Wireshark introduction ..

- Filters examples:
  - Tcp, http, … lists packts related to the said protocol
  - http.request.method == "GET“
  - ip.addr == ‘ip you’re looking for’
  - Check the “Hypertext Transfer Protocol” section

Questions?