

Pandit Deendayal Energy University
School of Technology
Department of ICT
Academic Year: 2022-23
Computer Communication and Networking Lab
20IC306P

Name: Jankar Patel

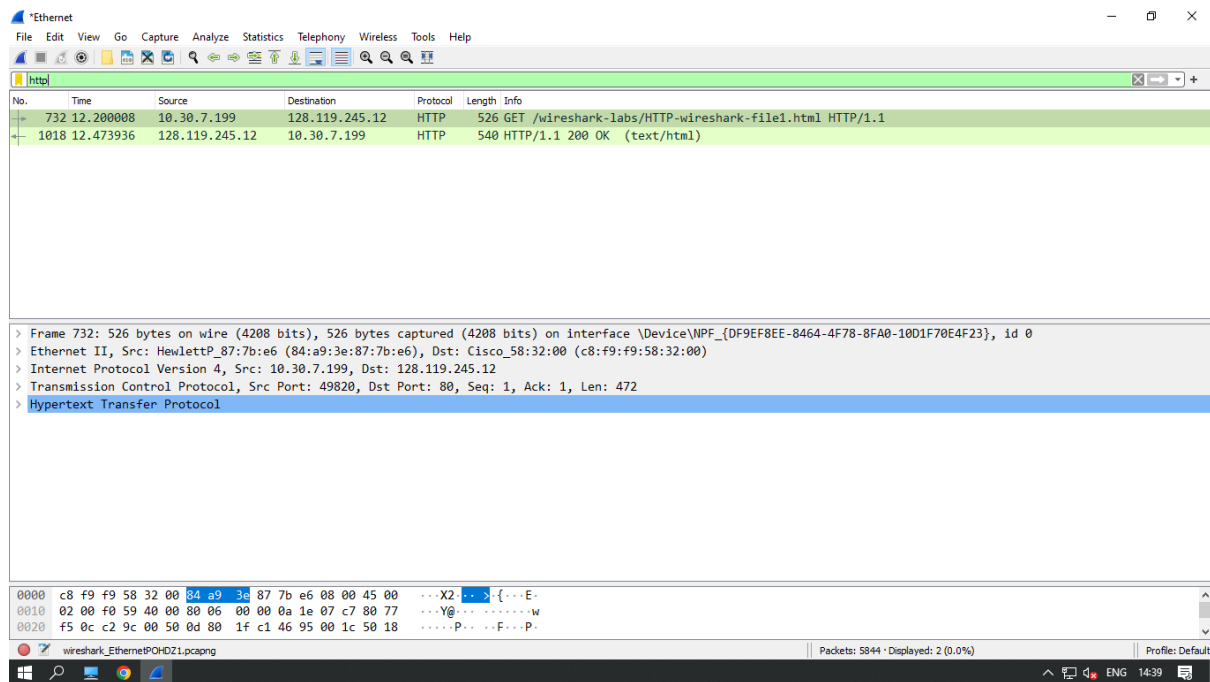
Roll No: 20BIT061

Experiment 3:

Aim: To understand the functionality of HTTP using Wire-shark and Packet Tracer

Software Tools required: - Wire-shark and Cisco packet tracer

Task 1: Understand HTTP and capture HTTP packets through wire-shark and analyse those packets. Answer all the questions. Write down notes and remarks for your reference whenever required.



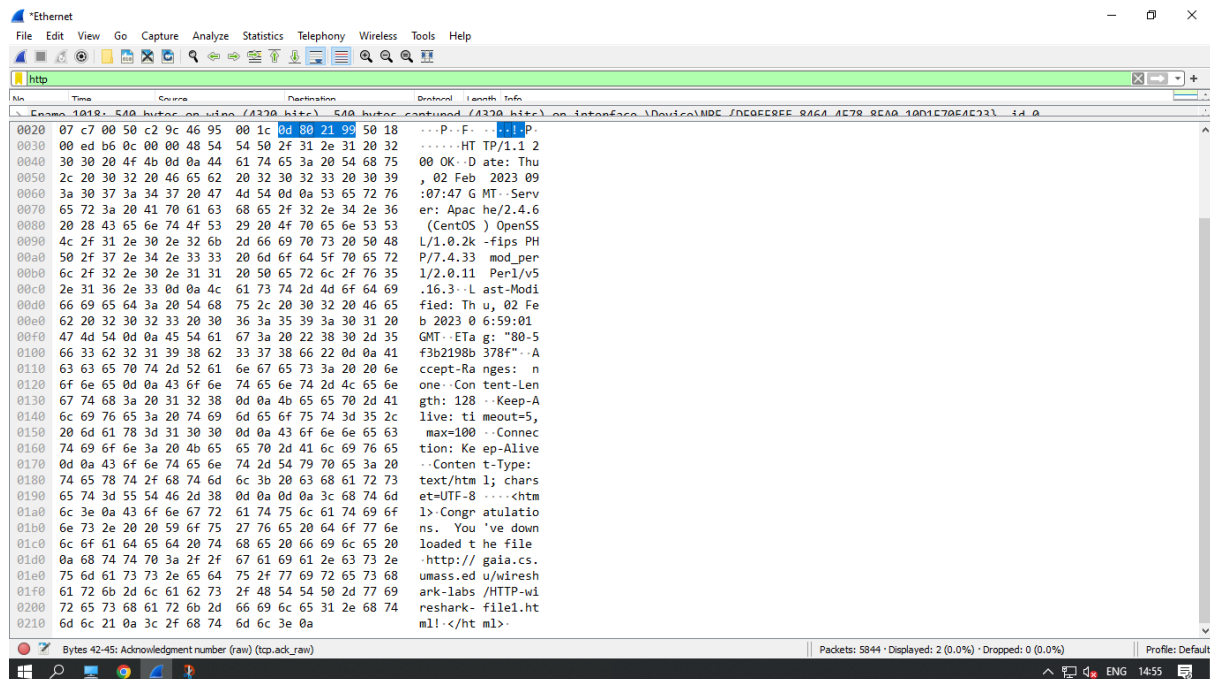
1. The Basic HTTP GET/response interaction

The screenshot shows the Wireshark interface with a packet capture of an HTTP GET request. The packet list pane shows a single packet (No. 732) at time 12.200008, source 10.30.7.199, destination 128.119.245.12, protocol HTTP, length 526, and info GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the request line, host, connection, upgrade-insecure-requests, user-agent, accept, accept-encoding, and accept-language headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark packet capture showing an HTTP GET request. The packet list pane shows a single packet (No. 732) at time 12.200008, source 10.30.7.199, destination 128.119.245.12, protocol HTTP, length 526, and info GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the request line, host, connection, upgrade-insecure-requests, user-agent, accept, accept-encoding, and accept-language headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

The screenshot shows the Wireshark interface with a packet capture of an HTTP 200 OK response. The packet list pane shows two packets: packet 732 (GET request) and packet 1018 (200 OK response) at time 12.473936, source 128.119.245.12, destination 10.30.7.199, protocol HTTP, length 540, and info HTTP/1.1 200 OK (text/html). The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the status line, date, server, last-modified, etag, accept-ranges, content-length, keep-alive, connection, and content-type headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Wireshark packet capture showing an HTTP 200 OK response. The packet list pane shows two packets: packet 732 (GET request) and packet 1018 (200 OK response) at time 12.473936, source 128.119.245.12, destination 10.30.7.199, protocol HTTP, length 540, and info HTTP/1.1 200 OK (text/html). The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the status line, date, server, last-modified, etag, accept-ranges, content-length, keep-alive, connection, and content-type headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.



1. Is your browser running HTTP version 1.0, 1.1, or 2? What version of HTTP is the server running?
Ans: Browser and the server both running on HTTP 1.1 Version.
2. What languages (if any) does your browser indicate that it can accept to the server?
Ans: It indicates that the server accepts the English US Language.
3. What is the IP address of your computer? What is the IP address of the gaia.cs.umass.edu server?
Ans: Computer IP Address: 10.30.7.199, Server IP Address: 128.119.245.12
4. What is the status code returned from the server to your browser?
Ans: Status Code 200 OK returned from the server.
5. When was the HTML file that you are retrieving last modified at the server?
Ans: HTML file was modified: Thursday, 02 Feb 2023 06:59:01 GMT.
6. How many bytes of content are being returned to your browser?
Ans: The length of content returned is 128 bytes.
7. By inspecting the raw data in the packet content window, do you see any headers within the data that are not displayed in the packet-listing window? If so, name one.
Ans: None, All the headers are visible.

2. The HTTP CONDITIONAL GET/response interaction

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
127	5.179376	10.30.7.199	128.119.245.12	HTTP	416	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141	5.482053	128.119.245.12	10.30.7.199	HTTP	784	HTTP/1.1 200 OK (text/html)
318	10.094155	10.30.7.199	128.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327	10.397855	128.119.245.12	10.30.7.199	HTTP	293	HTTP/1.1 304 Not Modified

The packet details pane for the selected packet (No. 327) shows the Hypertext Transfer Protocol section:

- GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
- Host: gaia.cs.umass.edu\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0\r\n

The packet bytes pane shows the raw data of the HTTP request.

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list pane displays four packets:

No.	Time	Source	Destination	Protocol	Length	Info
127	5.179376	10.30.7.199	128.119.245.12	HTTP	416	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141	5.482053	128.119.245.12	10.30.7.199	HTTP	784	HTTP/1.1 200 OK (text/html)
318	10.094155	10.30.7.199	128.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327	10.397855	128.119.245.12	10.30.7.199	HTTP	293	HTTP/1.1 304 Not Modified

The packet details pane for the selected packet (No. 327) shows the Hypertext Transfer Protocol section:

- GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
- Host: gaia.cs.umass.edu\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n

The packet bytes pane shows the raw data of the HTTP request.

Wireshark interface showing a packet capture on the Ethernet interface. The packet list shows five HTTP packets. The selected packet (No. 318) is an HTTP 200 OK response from 10.30.7.199 to 10.30.7.199. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the response body content. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
127	5.179376	10.30.7.199	128.119.245.12	HTTP	416	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141	5.482053	128.119.245.12	10.30.7.199	HTTP	784	HTTP/1.1 200 OK (text/html)
318	10.094155	10.30.7.199	128.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327	10.397855	128.119.245.12	10.30.7.199	HTTP	293	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Thu, 02 Feb 2023 09:48:32 GMT\r\n

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

Last-Modified: Thu, 02 Feb 2023 06:59:01 GMT\r\n

ETag: "173-5f3b2198b2fbc"\r\n

Accept-Ranges: none\r\n

Content-Length: 371\r\n

Keep-Alive: timeout=5, max=100\r\n

Connection: Keep-Alive\r\n

Content-Type: text/html; charset=UTF-8\r\n

\r\n

[HTTP response 1/2]

[Time since request: 0.302677000 seconds]

Wireshark interface showing a packet capture on the Ethernet interface. The packet list shows five HTTP packets. The selected packet (No. 318) is an HTTP 200 OK response from 10.30.7.199 to 10.30.7.199. The packet details pane shows the Hypertext Transfer Protocol section expanded, displaying the response body content. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
127	5.179376	10.30.7.199	128.119.245.12	HTTP	416	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
141	5.482053	128.119.245.12	10.30.7.199	HTTP	784	HTTP/1.1 200 OK (text/html)
318	10.094155	10.30.7.199	128.119.245.12	HTTP	528	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
327	10.397855	128.119.245.12	10.30.7.199	HTTP	293	HTTP/1.1 304 Not Modified

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:48.0) Gecko/20100101 Firefox/48.0\r\n

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n

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

Accept-Encoding: gzip, deflate\r\n

Connection: keep-alive\r\n

Upgrade-Insecure-Requests: 1\r\n

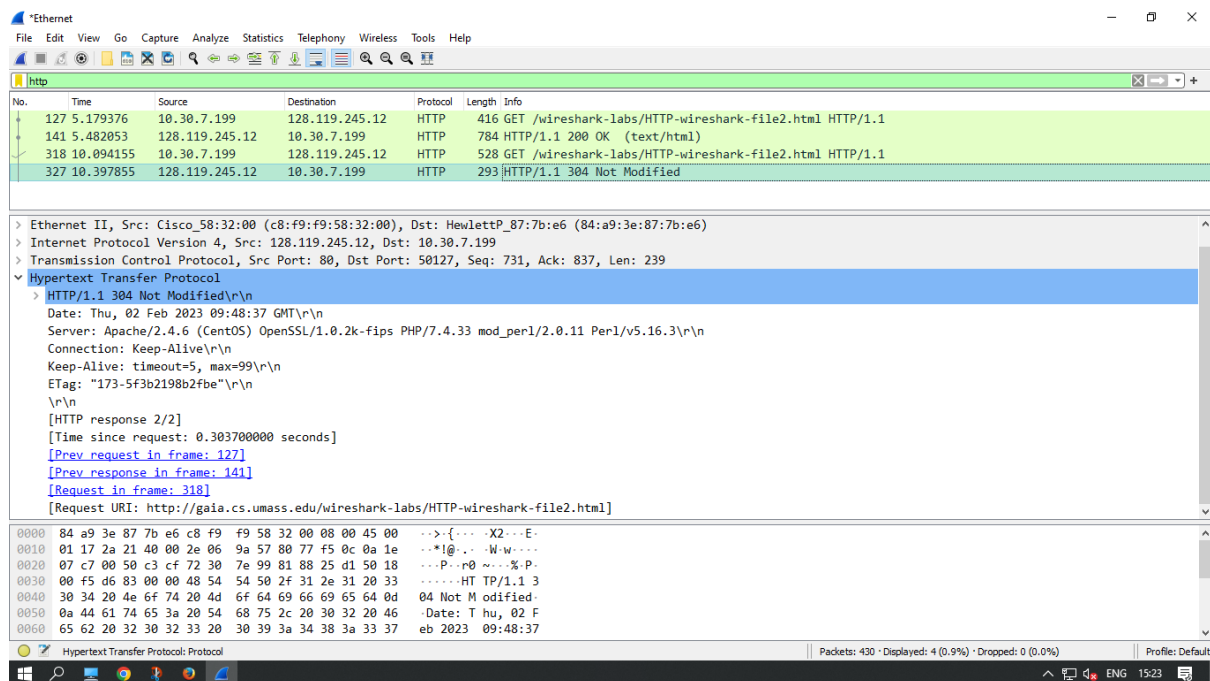
If-Modified-Since: Thu, 02 Feb 2023 06:59:01 GMT\r\n

If-None-Match: "173-5f3b2198b2fbc"\r\n

Cache-Control: max-age=0\r\n

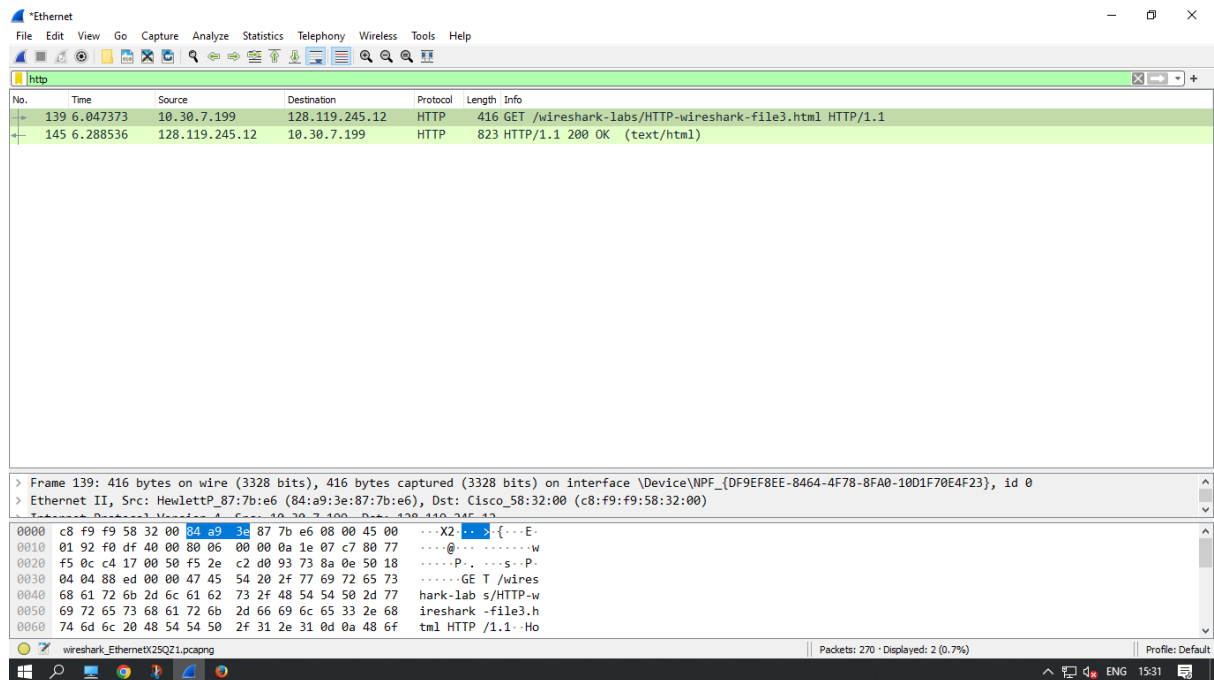
\r\n

[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]



8. Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE" line in the HTTP GET?
Ans: Yes, the line is present in the GET request. it consists Thu, 02 Feb 2023 06:59:01 GMT.
9. Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?
Ans: Server responded with code 200 OK status code.
10. Now inspect the contents of the second HTTP GET request from your browser to the server. Do you see an "IF-MODIFIED-SINCE:" line in the HTTP GET¹? If so, what information follows the "IF-MODIFIED-SINCE:" header?
Ans: Yes, The line is present in the second response, but it responded with 304 not modified status code.
11. What is the HTTP status code and phrase returned from the server in response to this second HTTP GET? Did the server explicitly return the contents of the file? Explain.
Ans: In the second response server responded with 304 NOT MODIFIED code. server is not returning explicitly.

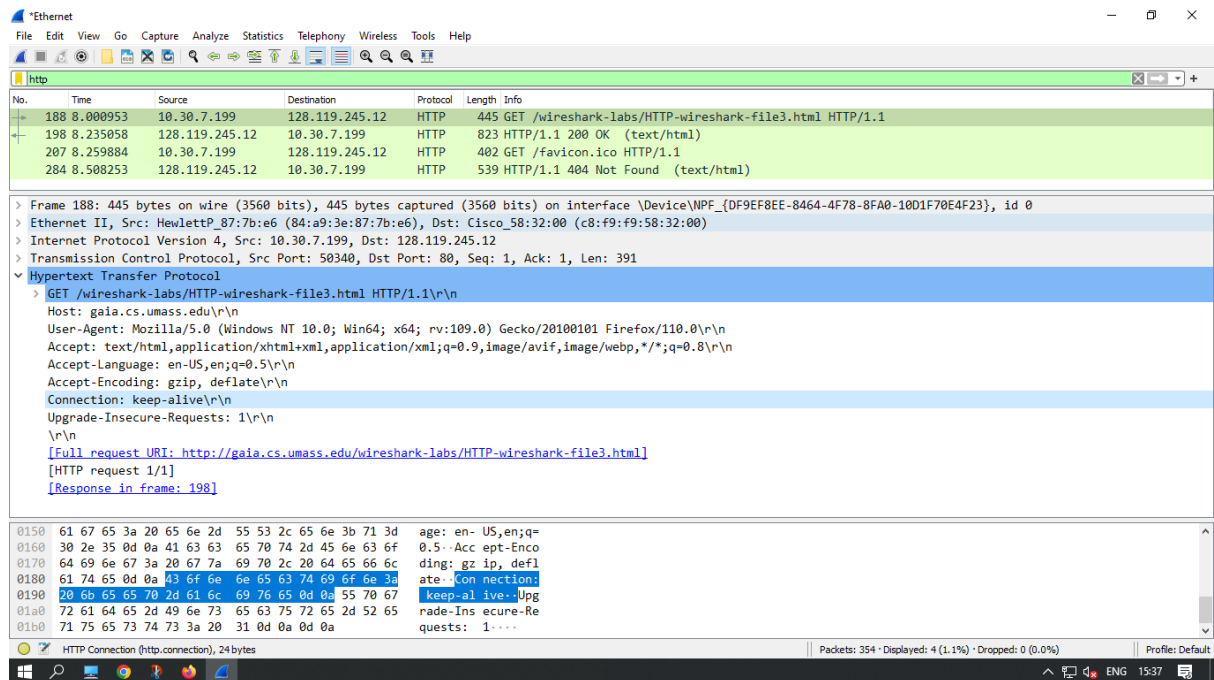
3. Retrieving Long Documents



The screenshot shows the Wireshark interface with a capture on the 'Ethernet' interface. The packet list shows two packets: a GET request (No. 139) and its response (No. 145). The packet details pane shows the 'Hypertext Transfer Protocol' section expanded, displaying the request line: 'GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1'. The packet bytes pane shows the raw data of the request, including the host 'gaia.cs.umass.edu' and the user agent 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0'.

No.	Time	Source	Destination	Protocol	Length	Info
139	6.047373	10.30.7.199	128.119.245.12	HTTP	416	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
145	6.288536	128.119.245.12	10.30.7.199	HTTP	823	HTTP/1.1 200 OK (text/html)

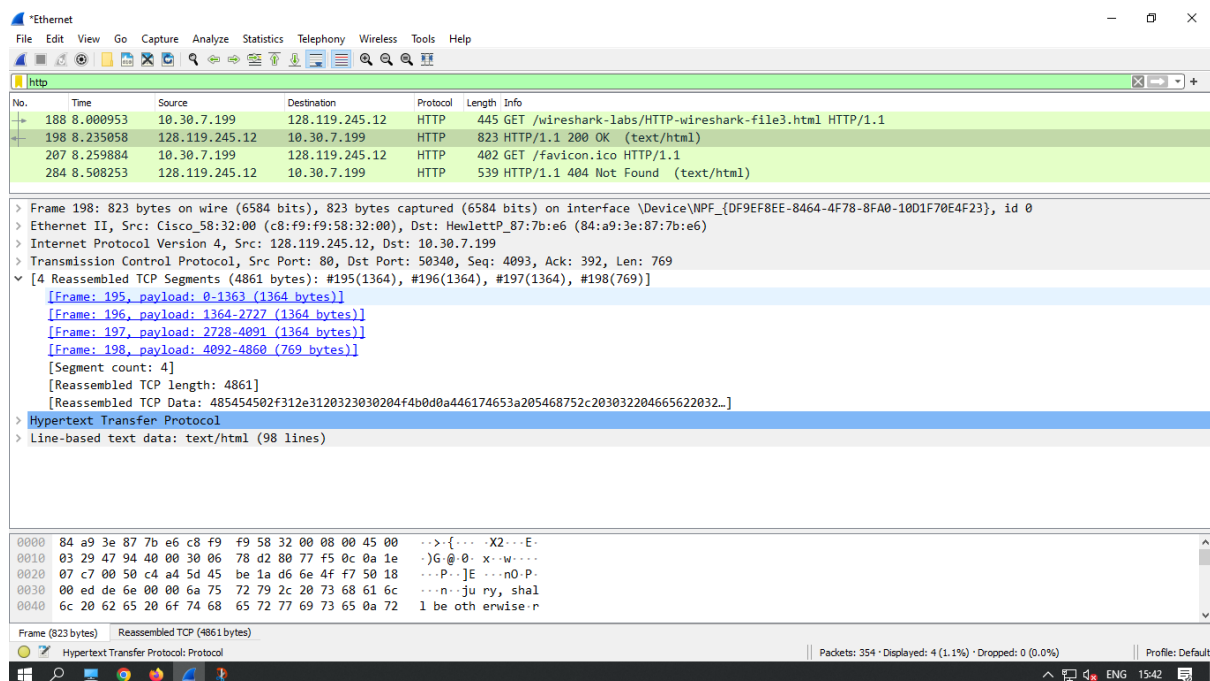
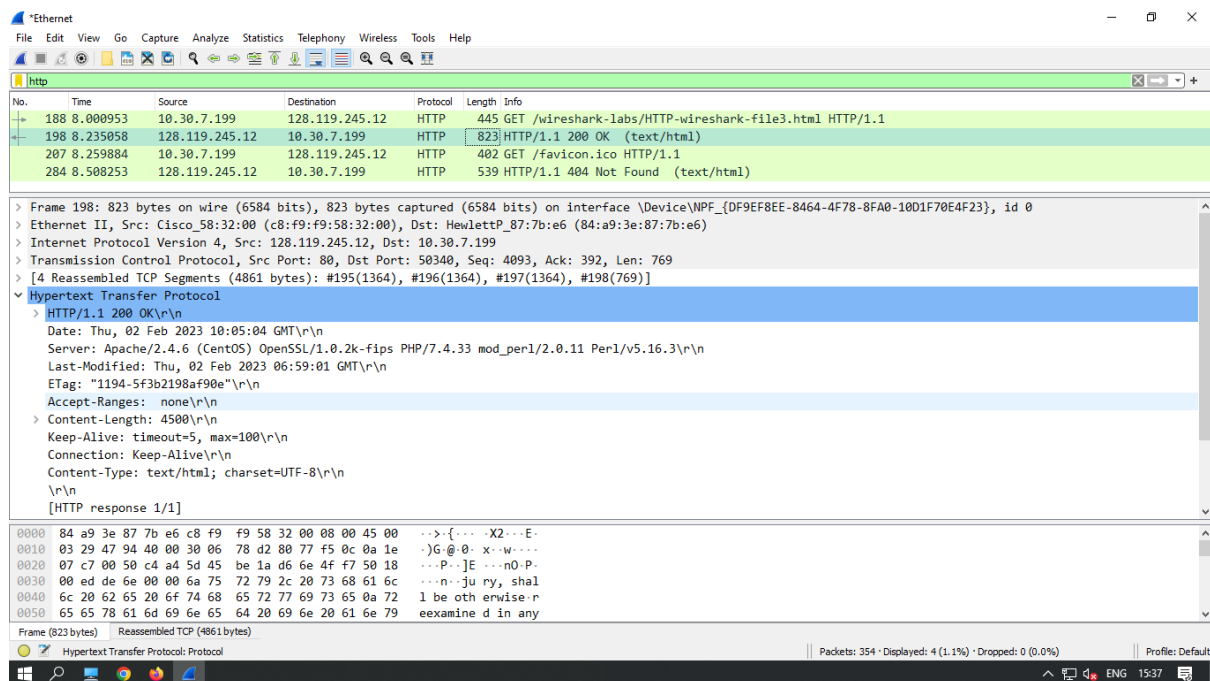
Frame 139: 416 bytes on wire (3328 bits), 416 bytes captured (3328 bits) on interface \Device\NPF_{DF9EF8EE-8464-4F78-8FA0-10D1F70E4F23}, id 0
> Ethernet II, Src: HewlettP_87:7b:e6 (84:a9:3e:87:7b:e6), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
> Internet Protocol Version 4, Src: 10.30.7.199, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50340, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
[Response in frame: 198]



The screenshot shows the Wireshark interface with a capture on the 'Ethernet' interface. The packet list shows four packets: a GET request (No. 188), its response (No. 198), a GET request for a favicon (No. 207), and its response (No. 284). The packet details pane shows the 'Hypertext Transfer Protocol' section expanded, displaying the request line: 'GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1'. The packet bytes pane shows the raw data of the request, including the host 'gaia.cs.umass.edu' and the user agent 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0'.

No.	Time	Source	Destination	Protocol	Length	Info
188	8.000953	10.30.7.199	128.119.245.12	HTTP	445	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
198	8.235058	128.119.245.12	10.30.7.199	HTTP	823	HTTP/1.1 200 OK (text/html)
207	8.259884	10.30.7.199	128.119.245.12	HTTP	402	GET /favicon.ico HTTP/1.1
284	8.508253	128.119.245.12	10.30.7.199	HTTP	539	HTTP/1.1 404 Not Found (text/html)

Frame 188: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\NPF_{DF9EF8EE-8464-4F78-8FA0-10D1F70E4F23}, id 0
> Ethernet II, Src: HewlettP_87:7b:e6 (84:a9:3e:87:7b:e6), Dst: Cisco_58:32:00 (c8:f9:f9:58:32:00)
> Internet Protocol Version 4, Src: 10.30.7.199, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 50340, Dst Port: 80, Seq: 1, Ack: 1, Len: 391
> Hypertext Transfer Protocol
> GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1\r\nHost: gaia.cs.umass.edu\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\n\r\n[Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html]
[HTTP request 1/1]
[Response in frame: 198]



Answer the following questions²:

12. How many HTTP GET request messages did your browser send? Which packet number in the trace contains the GET message for the Bill or Rights?
 Ans: One GET request is sent to the server. Packet number is 188.
13. Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

Ans: Packet number is 198.

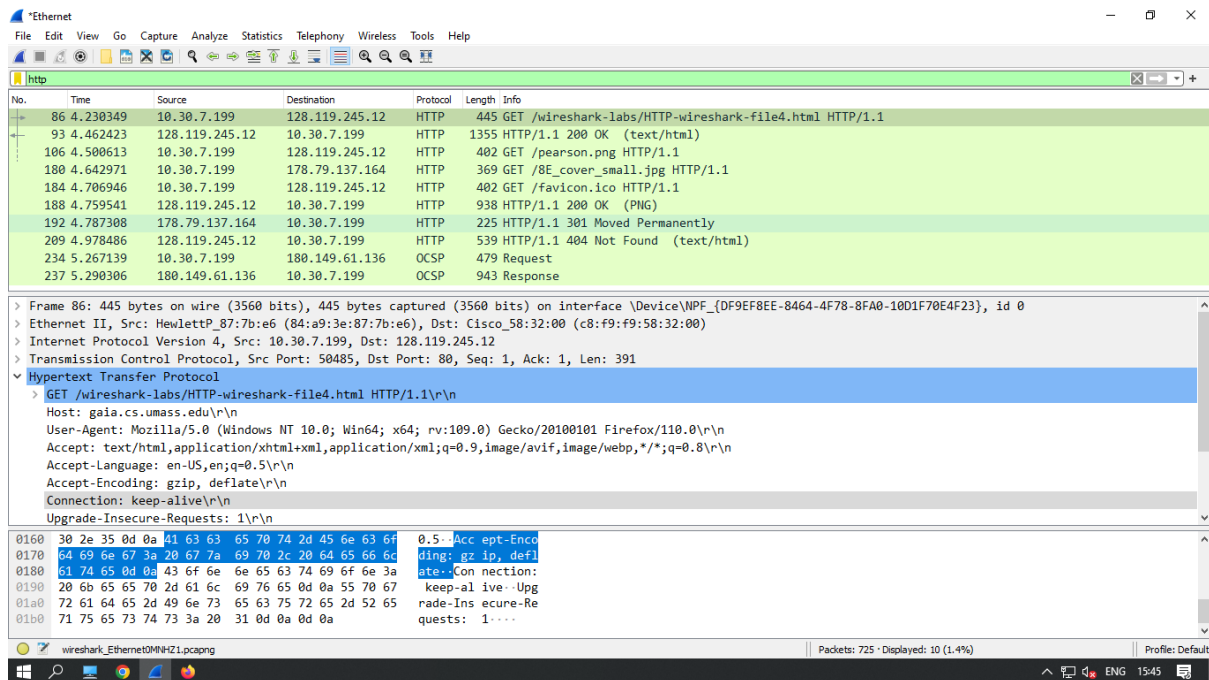
14. What is the status code and phrase in the response?

Ans: Status code 200 OK in response.

15. How many data-containing TCP segments were needed to carry the single HTTP response and the text of the Bill of Rights?

Ans: 4 TCP segments carry single HTTP.

4. HTML Documents with Embedded Objects



Answer the following questions³:

16. How many HTTP GET request messages did your browser send? To which Internet addresses were these GET requests sent?

Ans: Three HTTP GET requests are sent. Address are 128.119.245.12, 178.79.137.164

17. Can you tell whether your browser downloaded the two images serially, or whether they were downloaded from the two websites in parallel? Explain.

Ans: Downloaded Parallel.

5 HTTP Authentication

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list displays several HTTP requests and responses. The first GET request (No. 69) for `/wireshark-labs/protected_pages/HTTP-wireshark-file5.html` receives a 401 Unauthorized response. The second GET request (No. 924) includes an Authorization header and receives a 200 OK response. The third GET request (No. 941) for `/favicon.ico` receives a 404 Not Found response.

No.	Time	Source	Destination	Protocol	Length	Info
69	5.091127	10.30.7.199	128.119.245.12	HTTP	461	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
76	5.339550	128.119.245.12	10.30.7.199	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
919	40.788957	10.30.7.199	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
924	41.030468	128.119.245.12	10.30.7.199	HTTP	544	HTTP/1.1 200 OK (text/html)
941	41.075836	10.30.7.199	128.119.245.12	HTTP	418	GET /favicon.ico HTTP/1.1
1002	41.315468	128.119.245.12	10.30.7.199	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for the selected packet (No. 924) shows the following fields:

- GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
- Host: gaia.cs.umass.edu\r\n
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n

The packet bytes pane shows the raw data of the request, including the Authorization header: `Authorization: Basic d2lyZXNoYXJnLXN0dWR1bnRzM05ldHdvcms=`.

The screenshot shows a Wireshark packet capture on an Ethernet interface. The packet list displays several HTTP requests and responses. The first GET request (No. 69) for `/wireshark-labs/protected_pages/HTTP-wireshark-file5.html` receives a 401 Unauthorized response. The second GET request (No. 924) includes an Authorization header and receives a 200 OK response. The third GET request (No. 941) for `/favicon.ico` receives a 404 Not Found response.

No.	Time	Source	Destination	Protocol	Length	Info
69	5.091127	10.30.7.199	128.119.245.12	HTTP	461	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
76	5.339550	128.119.245.12	10.30.7.199	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
919	40.788957	10.30.7.199	128.119.245.12	HTTP	520	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
924	41.030468	128.119.245.12	10.30.7.199	HTTP	544	HTTP/1.1 200 OK (text/html)
941	41.075836	10.30.7.199	128.119.245.12	HTTP	418	GET /favicon.ico HTTP/1.1
1002	41.315468	128.119.245.12	10.30.7.199	HTTP	538	HTTP/1.1 404 Not Found (text/html)

The packet details pane for the selected packet (No. 924) shows the following fields:

- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/110.0\r\n
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
- Accept-Language: en-US,en;q=0.5\r\n
- Accept-Encoding: gzip, deflate\r\n
- Connection: keep-alive\r\n
- Upgrade-Insecure-Requests: 1\r\n
- Authorization: Basic d2lyZXNoYXJnLXN0dWR1bnRzM05ldHdvcms=\r\n
- Credentials: wireshark-students:network\r\n
- [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
- [HTTP request 1/2]
- [Response in frame: 924]
- [Next request in frame: 941]

The packet bytes pane shows the raw data of the request, including the Authorization header: `Authorization: Basic d2lyZXNoYXJnLXN0dWR1bnRzM05ldHdvcms=`.

Answer the following questions9:

18. What is the server's response (status code and phrase) in response to the initial HTTP GET message from your browser?

Ans: 401 Unauthorized and 200 OK status code.

19. When your browser sends the HTTP GET message for the second time, what new field is included in the HTTP GET message?

Ans: Authorization.

Task 2: Configure a web server and use HTTP in packet tracer. Use a step by step approach with proper understanding of each step.

