

RESOLUÇÃO DO 3º LABORATORIO DE REDES E COMPUTADORES I

Feito por: Rodrigo Linhas a83933

2º ano da Licenciatura de Engenharia Informática
(LEI)

Regente da UC: Noélia Correia

Ano letivo 2024/2025

ÍNDICE

Introdução.....	3
Domínio 1.....	4
Pergunta 1	4
Pergunta 2	4
Pergunta 3	5
Pergunta 4	5
Pergunta 5	6
Pergunta 6	6
Pergunta 7	7
Domínio 2.....	8
Pergunta 8	8
Pergunta 9	8
Pergunta 10.....	9
Pergunta 11.....	9
Domínio 3.....	10
Pergunta 12.....	10
Pergunta 13.....	11
Pergunta 14.....	11
Pergunta 15.....	11
Domínio 4.....	12
Pergunta 16.....	12
Pergunta 17.....	12
Domínio 5.....	13
Pergunta 18.....	13
Pergunta 19.....	13

Introdução

Este documento tem o intuito de demonstrar a minha resolução das perguntas propostas do enunciado¹ do 3º laboratório da cadeira de redes 1.

O enunciado tem 5 grandes domínios e cada um com várias perguntas, foi necessário também para a resolução das perguntas a utilização da ferramenta Wireshark².

A estrutura deste documento tem o seguinte aspeto:

Domínio

Pergunta

Resposta

Captura de ecrã (se for necessário)

¹ https://tutoria.ualg.pt/2024/pluginfile.php/206691/mod_resource/content/1/Wireshark_HTTP_v7.0.pdf

² <https://www.wireshark.org/>

Domínio 1

Para o domínio 1 foi necessário aceder o seguinte site enquanto se fazia a captura no Wireshark: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html>

Pergunta 1

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

R: O browser tem o HTTP 1.1. O server também tem o HTTP 1.1

(Após ter consultado o GET/OK->Hypertext->Request Version)

```

2290 15:24:31.355811 10.20.76.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307 15:24:31.495607 128.119.245.12 10.20.76.93 HTTP 540 HTTP/1.1 200 OK (text/html)
2310 15:24:31.532264 10.20.76.93 128.119.245.12 HTTP 482 GET /favicon.ico HTTP/1.1
2332 15:24:31.686305 128.119.245.12 10.20.76.93 HTTP 538 HTTP/1.1 404 Not Found (text/html)

Frame 2290: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface \Device\NPF...
Ethernet II, Src: CloudNetwork_88:80:a5 (ac:50:de:88:80:a5), Dst: HuaweiTechno_9b:52:f4 (04:f9:38:9b:52)
Internet Protocol Version 4, Src: 10.20.76.93, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50219, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
Hypertext Transfer Protocol
  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
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101 Firefox/135.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: pt-PT;q=0.8,en;q=0.5,en-US;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
  
```

Pergunta 2

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

R: O browser está em pt-PT e em en-US, no entanto a língua pt-PT é a dominante uma vez que aparece primeiro

(Após ter consultado o GET -> o header Hypertext -> Accept-Language)

```

2290 15:24:31.355811 10.20.76.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307 15:24:31.495607 128.119.245.12 10.20.76.93 HTTP 540 HTTP/1.1 200 OK (text/html)
2310 15:24:31.532264 10.20.76.93 128.119.245.12 HTTP 482 GET /favicon.ico HTTP/1.1
2332 15:24:31.686305 128.119.245.12 10.20.76.93 HTTP 538 HTTP/1.1 404 Not Found (text/html)

Frame 2290: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface \Device\NPF...
Ethernet II, Src: CloudNetwork_88:80:a5 (ac:50:de:88:80:a5), Dst: HuaweiTechno_9b:52:f4 (04:f9:38:9b:52)
Internet Protocol Version 4, Src: 10.20.76.93, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 50219, Dst Port: 80, Seq: 1, Ack: 1, Len: 408
Hypertext Transfer Protocol
  GET /wireshark-labs/HTTP-wireshark-file1.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:135.0) Gecko/20100101 Firefox/135.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: pt-PT;q=0.8,en;q=0.5,en-US;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
  
```

Pergunta 3

What is the IP address of your computer? Of the gaia.cs.umass.edu server?

R: O meu IP: 10.20.76.93 e o IP do servidor: 128.119.245.12 (Apos ter visto o IP source e destination do GET)

No.	Time	Source	Destination	Protocol	Length	Info
481	15:24:22,431076	10.20.76.93	194.210.238.81	OCSP	516	Request
488	15:24:22,450688	194.210.238.81	10.20.76.93	OCSP	943	Response
501	15:24:22,457715	34.107.221.82	10.20.76.93	HTTP	270	HTTP/1.1 200 OK (text/plain)
516	15:24:22,481063	194.210.238.81	10.20.76.93	OCSP	944	Response
606	15:24:22,760876	10.20.76.93	34.107.221.82	HTTP	395	GET /success.txt?ipv4 HTTP/1.1
634	15:24:22,811237	142.250.185.3	10.20.76.93	OCSP	1157	Response
681	15:24:22,950268	34.107.221.82	10.20.76.93	HTTP	270	HTTP/1.1 200 OK (text/plain)
824	15:24:23,093189	10.20.76.93	194.210.238.81	OCSP	516	Request
825	15:24:23,183407	10.20.76.93	23.40.158.218	OCSP	516	Request
861	15:24:23,245956	10.20.76.93	23.40.158.218	OCSP	516	Request
862	15:24:23,246180	10.20.76.93	194.210.238.81	OCSP	516	Request
864	15:24:23,255333	194.210.238.81	10.20.76.93	OCSP	944	Response
869	15:24:23,255333	23.40.158.218	10.20.76.93	OCSP	926	Response
872	15:24:23,255639	10.20.76.93	194.210.238.81	OCSP	516	Request
894	15:24:23,306754	194.210.238.81	10.20.76.93	OCSP	944	Response
901	15:24:23,329542	23.40.158.218	10.20.76.93	OCSP	929	Response
927	15:24:23,410392	194.210.238.81	10.20.76.93	OCSP	944	Response
2290	15:24:31,355811	10.20.76.93	128.119.245.12	HTTP	462	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307	15:24:31,495607	128.119.245.12	10.20.76.93	HTTP	540	HTTP/1.1 200 OK (text/html)
2310	15:24:31,532264	10.20.76.93	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
2332	15:24:31,686305	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Pergunta 4

What is the status code returned from the server to your browser?

R: Status Code: 200 OK (Apos ter consultado o OK -> Hypertext > Status Code)

2290	15:24:31,355811	10.20.76.93	128.119.245.12	HTTP	462	GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307	15:24:31,495607	128.119.245.12	10.20.76.93	HTTP	540	HTTP/1.1 200 OK (text/html)
2310	15:24:31,532264	10.20.76.93	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
2332	15:24:31,686305	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

<pre> Frame 2307: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF... Ethernet II, Src: HuaweiTechno_38:b7:90 (64:3e:8c:38:b7:90), Dst: CloudNetwork_B8:80:a5 (ac:50:de:88:80:a5) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.20.76.93 Transmission Control Protocol, Src Port: 80, Dst Port: 50219, Seq: 1, Ack: 409, Len: 486 Hypertext Transfer Protocol HTTP/1.1 200 OK\r\n Response Version: HTTP/1.1 Status Code: 200 [Status Code Description: OK] Response Phrase: OK Date: Mon, 24 Feb 2025 15:24:29 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 Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT\r\n ETag: "00-62edde008169e"\r\n Accept-Ranges: bytes\r\n Content-Length: 128\r\n Keep-Alive: timeout=5, max=100\r\n Connection: Keep-Alive\r\n </pre>	<pre> 0030 00 ed 3e 90 00 00 48 54 54 50 2f 31 2e 31 20 32 20 00 OK -D ate: Mon 0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e 00 OK -D ate: Mon 0050 2c 20 32 34 20 46 65 62 20 32 30 32 35 20 31 35 24 Feb 2025 15 0060 3a 32 34 3a 32 39 20 47 4d 54 0d 0a 53 65 72 76 :24:29 GMT..Serv 0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apache/2.4.6 0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 52 (CentOS) OpenSS 0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH 00a0 50 2f 37 2e 34 2e 33 33 20 6d 6f 64 5f 70 65 72 P/7.4.33 mod_per 00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 l/2.0.11 Perl/v5 00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3..l ast-Modi 00d0 66 69 65 64 3a 20 4d 6f 6e 2c 20 32 34 20 46 65 Filed: Mon, 24 Fe 00e0 62 20 32 30 32 35 20 30 36 3a 35 39 3a 30 31 20 b 2025 0 6:59:01 00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT--Etag: "00-6 0100 32 65 64 64 65 30 30 38 31 36 39 65 22 0d 0a 41 2edde008169e"..A 0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ranges: by 0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes..Content-Len 0130 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 ..Keep-A 0140 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5, 0150 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 ..Conne </pre>
---	--

Pergunta 5

When was the HTML file that you are retrieving last modified at the server?

R: 24 Fevereiro 2025 às 06:59:01 (Apos ter consultado o OK -> Hypertext -> Last-Modified)

```

2290 15:24:31.355811 10.20.76.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307 15:24:31.495607 128.119.245.12 10.20.76.93 HTTP 540 HTTP/1.1 200 OK (text/html)
2310 15:24:31.532264 10.20.76.93 128.119.245.12 HTTP 482 GET /favicon.ico HTTP/1.1
2332 15:24:31.686305 128.119.245.12 10.20.76.93 HTTP 538 HTTP/1.1 404 Not Found (text/html)

Frame 2307: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF...
Ethernet II, Src: HuaweiTechno_38:b7:90 (64:3e:8c:38:b7:90), Dst: CloudNetwork_88:80:a5 (ac:50:de:88:80:a5)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.20.76.93
Transmission Control Protocol, Src Port: 80, Dst Port: 50219, Seq: 1, Ack: 409, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 24 Feb 2025 15:24:29 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
  Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT\r\n
  ETag: "80-62edde008169e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\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
[Request in frame 2290]
[Time since request: 0.130796000 seconds]
0000 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 .16.3-Last-Modi
0008 56 89 65 64 3a 20 4d 6f 6e 2c 20 32 34 20 46 65 fied: Mo n, 24 fe
0016 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 b-2025 0 6:59:01
0024 32 65 64 64 65 30 30 38 31 36 39 65 22 0d 0a 41 GMT-ETag: "80-6
0032 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 2edde008169e"-A
0040 74 65 73 0d 0a 43 6f 6e 74 65 74 2d 54 79 70 65 3a 20 ccept-Ra nges: by
0048 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c tes-Content-Len
0056 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 gth: 128 --keep-A
0064 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 live: ti meout=5,
0072 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 max=100 --Conne
0080 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 tion: Ke ep-Alive
0088 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d --Conten t-Type:
0096 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f text/htm l; char
0104 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e et=UTF-8 ---<htm
0112 0c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 l> Congr atulatio
0120 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e ns. You 've down
0128 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 loaded t he file
0136 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 http:// gaia.cs.
0144 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 umass.ed u/wiresh
0152 6d 6c 21 0a 3c 2f 68 74 6d 6c 6e 3e 0a ark-labs /HTTP-wi
0160 0000 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT-ETag: "80-6
0168 32 65 64 64 65 30 30 38 31 36 39 65 22 0d 0a 41 2edde008169e"-A
0176 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
0184 74 65 73 0d 0a 43 6f 6e 74 65 74 2d 4c 65 6e tes-Content-Len
0192 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 --keep-A
0200 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
0208 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 --Conne
0216 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0224 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 --Conten t-Type:
0232 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; char
0240 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8 ---<htm
0248 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l> Congr atulatio
0256 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down
0264 0c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 loaded t he file
0272 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e http:// gaia.cs.
0280 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 umass.ed u/wiresh
0288 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 ark-labs /HTTP-wi
0296 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 reshark- file1.ht
0304 6d 6c 21 0a 3c 2f 68 74 6d 6c 6e 3e 0a ml! </ht ml>

```

Pergunta 6

How many bytes of content are being returned to your browser?

R: 128 bytes (Apos ter consultado o OK -> Hypertext -> Content-Length -> Content-Lenght)

```

2290 15:24:31.355811 10.20.76.93 128.119.245.12 HTTP 462 GET /wireshark-labs/HTTP-wireshark-file1.html HTTP/1.1
2307 15:24:31.495607 128.119.245.12 10.20.76.93 HTTP 540 HTTP/1.1 200 OK (text/html)
2310 15:24:31.532264 10.20.76.93 128.119.245.12 HTTP 482 GET /favicon.ico HTTP/1.1
2332 15:24:31.686305 128.119.245.12 10.20.76.93 HTTP 538 HTTP/1.1 404 Not Found (text/html)

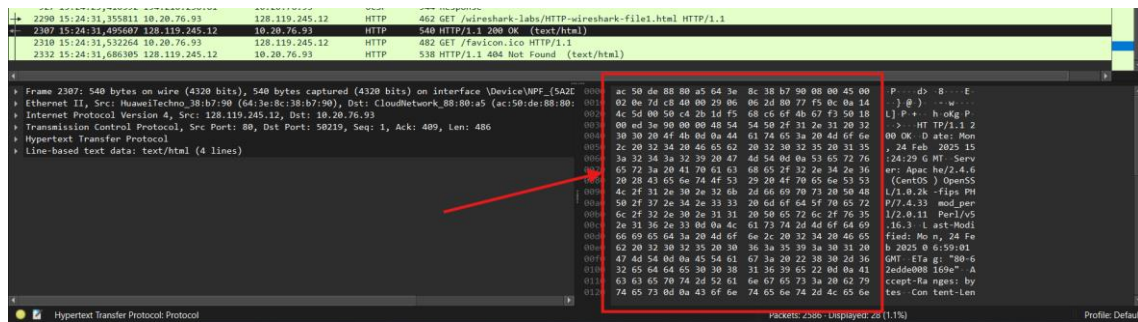
Frame 2307: 540 bytes on wire (4320 bits), 540 bytes captured (4320 bits) on interface \Device\NPF...
Ethernet II, Src: HuaweiTechno_38:b7:90 (64:3e:8c:38:b7:90), Dst: CloudNetwork_88:80:a5 (ac:50:de:88:80:a5)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.20.76.93
Transmission Control Protocol, Src Port: 80, Dst Port: 50219, Seq: 1, Ack: 409, Len: 486
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Mon, 24 Feb 2025 15:24:29 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
  Last-Modified: Mon, 24 Feb 2025 06:59:01 GMT\r\n
  ETag: "80-62edde008169e"\r\n
  Accept-Ranges: bytes\r\n
  Content-Length: 128\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
[Request in frame 2290]
[Time since request: 0.130796000 seconds]
0000 47 4d 54 0d 0a 45 54 61 67 3a 20 22 38 30 2d 36 GMT-ETag: "80-6
0008 32 65 64 64 65 30 30 38 31 36 39 65 22 0d 0a 41 2edde008169e"-A
0016 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ra nges: by
0024 74 65 73 0d 0a 43 6f 6e 74 65 74 2d 4c 65 6e tes-Content-Len
0032 67 74 68 3a 20 31 32 38 0d 0a 4b 65 65 70 2d 41 gth: 128 --keep-A
0040 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 2c live: ti meout=5,
0048 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 63 max=100 --Conne
0056 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive
0064 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 --Conten t-Type:
0072 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; char
0080 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 6d et=UTF-8 ---<htm
0088 6c 3e 0a 43 6f 6e 67 72 61 74 75 6c 61 74 69 6f l> Congr atulatio
0096 6e 73 2e 20 20 59 6f 75 27 76 65 20 64 6f 77 6e ns. You 've down
0104 0c 6f 61 64 65 64 20 74 68 65 20 66 69 6c 65 20 loaded t he file
0112 0a 68 74 74 70 3a 2f 2f 67 61 69 61 2e 63 73 2e http:// gaia.cs.
0120 75 6d 61 73 73 2e 65 64 75 2f 77 69 72 65 73 68 umass.ed u/wiresh
0128 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 77 69 ark-labs /HTTP-wi
0136 72 65 73 68 61 72 6b 2d 66 69 6c 65 31 2e 68 74 reshark- file1.ht
0144 6d 6c 21 0a 3c 2f 68 74 6d 6c 6e 3e 0a ml! </ht ml>

```

Pergunta 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.

R: Está a ser tudo bem interpretado porque ao andar pelas mensagem, o código hexadecimal vai ser de seguida o que significa que tudo está a ser interpretado (Apos ter consultado o código hexadecimal do OK)



Domínio 2

Para o domínio 2 foi necessário aceder o seguinte site enquanto se fazia a captura no Wireshark: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

Pergunta 8

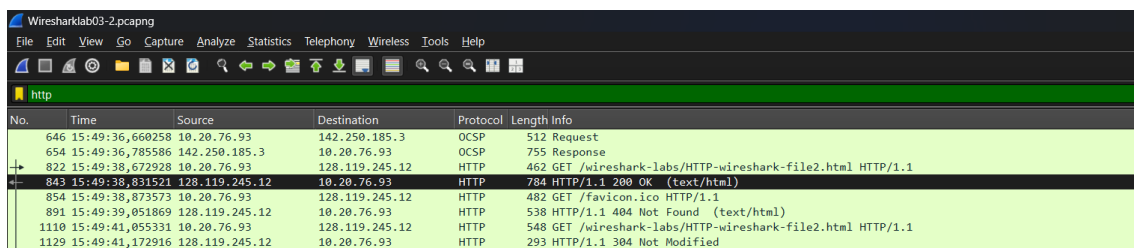
Inspect the contents of the first HTTP GET request from your browser to the server. Do you see an “IF-MODIFIED-SINCE” line in the HTTP GET?

R: No 1o não se encontra o “IF-MODIFIED-SINCE”, uma vez que tínhamos a cache limpa

Pergunta 9

Inspect the contents of the server response. Did the server explicitly return the contents of the file? How can you tell?

R: Retornou um 200 OK, logo obtivemos 1 objeto



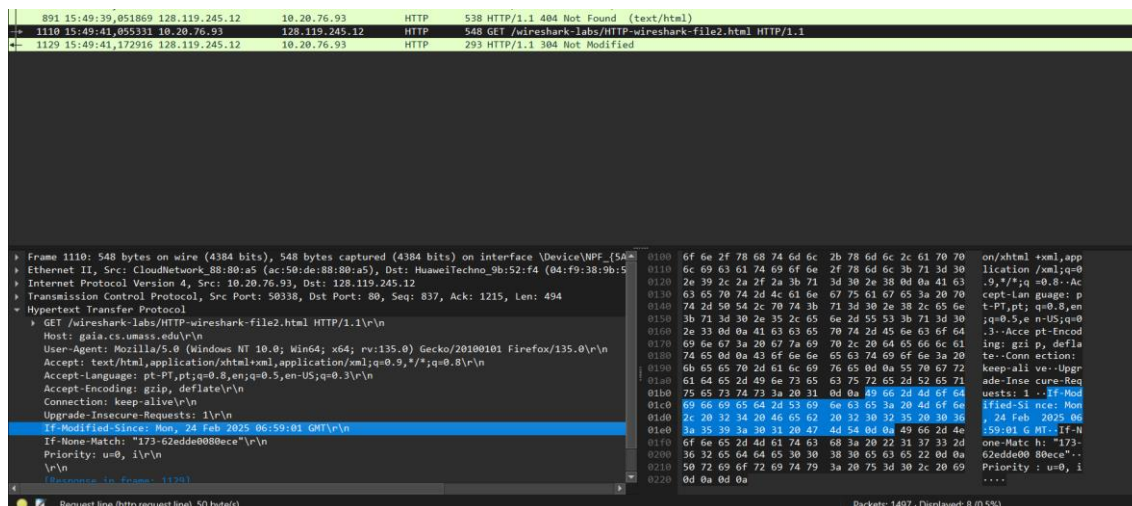
No.	Time	Source	Destination	Protocol	Length	Info
646	15:49:36,660258	10.20.76.93	142.250.185.3	OCSP	512	Request
654	15:49:36,785586	142.250.185.3	10.20.76.93	OCSP	755	Response
822	15:49:38,672928	10.20.76.93	128.119.245.12	HTTP	462	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
843	15:49:38,831521	128.119.245.12	10.20.76.93	HTTP	784	HTTP/1.1 200 OK (text/html)
854	15:49:38,873573	10.20.76.93	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
891	15:49:39,051869	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)
1110	15:49:41,055331	10.20.76.93	128.119.245.12	HTTP	548	GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
1129	15:49:41,172916	128.119.245.12	10.20.76.93	HTTP	293	HTTP/1.1 304 Not Modified

Pergunta 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 GET? If so, what information follows the “IF-MODIFIED-SINCE:” header?

R: Agora no 2o temos o “IF-MODIFIED-SINCE”, contendo a seguinte data:

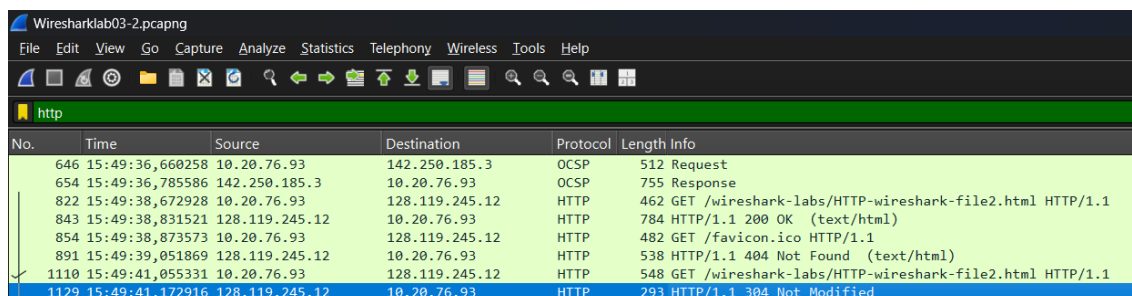
If-Modified-Since: Mon, 24 Feb 2025 06:59:01 GMT\r\n



Pergunta 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.

R: Recebemos o "304 - Not-Modified", implicando não necessitamos de receber o objeto, uma vez que está guardado na cache



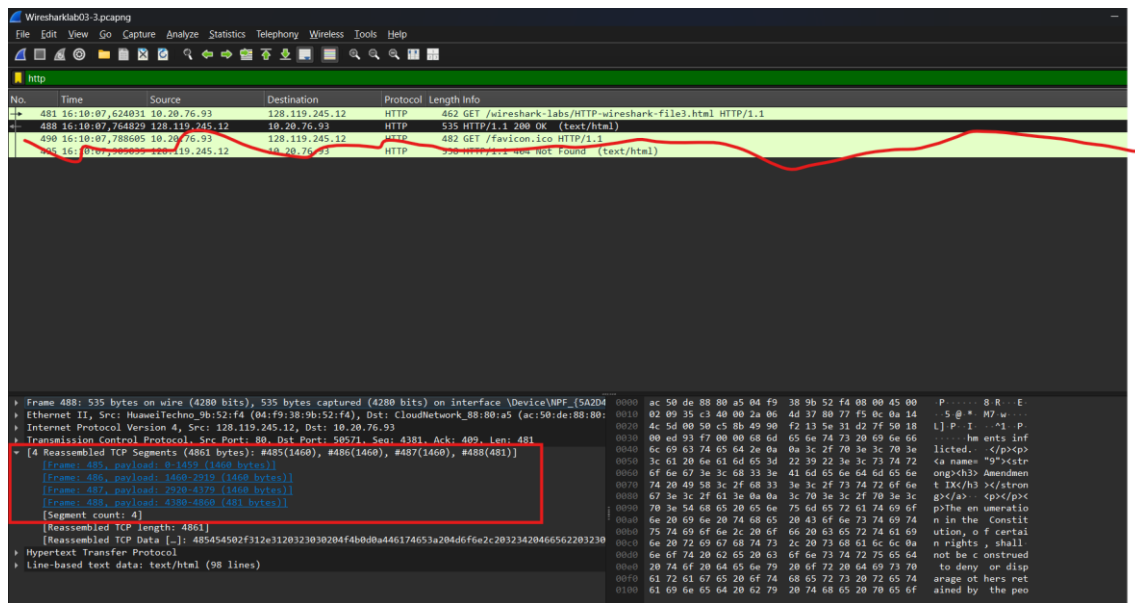
Domínio 3

Para o domínio 3 foi necessário aceder o seguinte site enquanto se fazia a captura no Wireshark: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>

Pergunta 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?

R: 1 GET , no entanto temos 4 pacotes que foram fragmentados no OK



Pergunta 13

Which packet number in the trace contains the status code and phrase associated with the response to the HTTP GET request?

R: É o pacote numero 485, foi o primeiro a ser recebido mas não foi transmitido, esse foi o ultimo pacote 488

No.	Time	Source	Destination	Protocol	Length	Info
481	16:10:07.624031	10.20.76.93	128.119.245.12	HTTP	462	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
488	16:10:07.764829	128.119.245.12	10.20.76.93	HTTP	535	HTTP/1.1 200 OK (text/html)
489	16:10:07.788605	10.20.76.93	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
495	16:10:07.905035	128.119.245.12	10.20.76.93	HTTP	535	HTTP/1.1 404 Not Found (text/html)

Frame	Offset	Length	Info
485	0-1459	1460	bytes
486	1460-2919	1460	bytes
487	2920-4379	1460	bytes
488	4380-4861	482	bytes

Pergunta 14

What is the status code and phrase in the response?

R: Retornou um 200 OK, mas obtivemos 4 pedacos de 1 objeto (uma vez que é muito grande)

Pergunta 15

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

R: 4 segmentos de TCP, sendo segmento1 /n segmento2 /n segmento3 /n segmento4 /n. O wireshark faz pensar que http é o último segmento mas na verdade é o 1º

Domínio 4

Para o domínio 4 foi necessário aceder o seguinte site enquanto se fazia a captura no Wireshark: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

Pergunta 16

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

R: Recebeu 3 GET's, 2 do 128.119.245.12 (entrar no site e a 1a imagem o logo) e 1 do 178.79.137.164 (recebe a imagem de uma ponte)

No.	Time	Source	Destination	Protocol	Length	Info
122	16:26:47,563530	10.20.76.93	128.119.245.12	HTTP	462	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
132	16:26:47,685177	128.119.245.12	10.20.76.93	HTTP	1355	HTTP/1.1 200 OK (text/html)
138	16:26:47,712471	10.20.76.93	128.119.245.12	HTTP	485	GET /pearson.png HTTP/1.1
146	16:26:47,780819	10.20.76.93	178.79.137.164	HTTP	452	GET /8E_cover_small.jpg HTTP/1.1
169	16:26:47,834145	128.119.245.12	10.20.76.93	HTTP	745	HTTP/1.1 200 OK (PNG)
172	16:26:47,849906	178.79.137.164	10.20.76.93	HTTP	225	HTTP/1.1 301 Moved Permanently
188	16:26:47,856495	10.20.76.93	128.119.245.12	HTTP	482	GET /favicon.ico HTTP/1.1
200	16:26:48,076423	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Pergunta 17

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

R: Foi sacado em paralelo, uma vez que houve 2 GET'S e por fim houve 2 OK's, implicando que foi em paralelo. Se fosse em serie seria GET OK GET OK.

Length	Info
462	GET /wireshark-labs/HTTP-wireshark-file4.html HTTP/1.1
1355	HTTP/1.1 200 OK (text/html)
485	GET /pearson.png HTTP/1.1
452	GET /8E_cover_small.jpg HTTP/1.1
745	HTTP/1.1 200 OK (PNG)
225	HTTP/1.1 301 Moved Permanently
482	GET /favicon.ico HTTP/1.1
538	HTTP/1.1 404 Not Found (text/html)

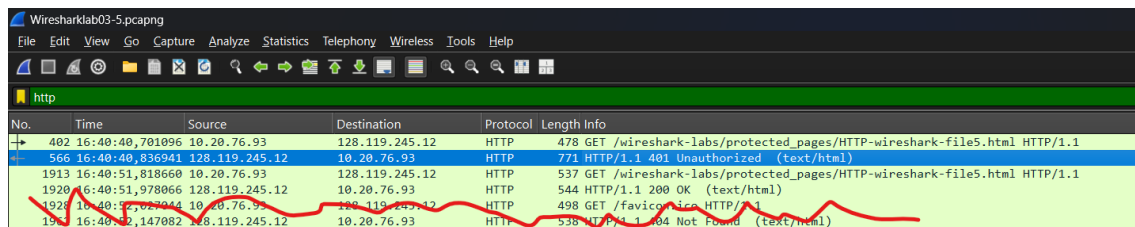
Domínio 5

Para o domínio 5 foi necessário aceder o seguinte site enquanto se fazia a captura no Wireshark: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file5.html>

Pergunta 18

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

R: A resposta do 1o GET foi 401 Unauthorized, implica que não tínhamos autorização para entrar, neste caso tínhamos de introduzir as credenciais



No.	Time	Source	Destination	Protocol	Length	Info
402	16:40:40,701096	10.20.76.93	128.119.245.12	HTTP	478	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
566	16:40:40,836941	128.119.245.12	10.20.76.93	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1913	16:40:51,818660	10.20.76.93	128.119.245.12	HTTP	537	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1920	16:40:51,978066	128.119.245.12	10.20.76.93	HTTP	544	HTTP/1.1 200 OK (text/html)
1928	16:40:52,027044	10.20.76.93	128.119.245.12	HTTP	498	GET /favicon.ico HTTP/1.1
1962	16:40:52,147082	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

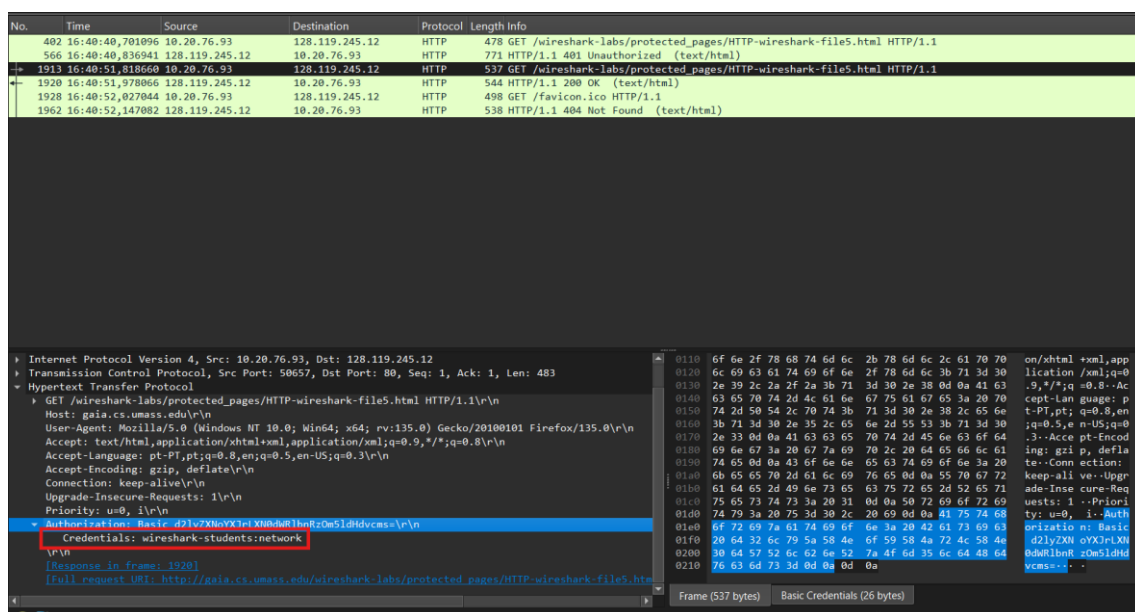
Pergunta 19

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

R: No segundo GET obtivemos um novo header dentro do HTTP que contem as credencias do login feito

Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=

Credentials: wireshark-students:network



No.	Time	Source	Destination	Protocol	Length	Info
402	16:40:40,701096	10.20.76.93	128.119.245.12	HTTP	478	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
566	16:40:40,836941	128.119.245.12	10.20.76.93	HTTP	771	HTTP/1.1 401 Unauthorized (text/html)
1913	16:40:51,818660	10.20.76.93	128.119.245.12	HTTP	537	GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1
1920	16:40:51,978066	128.119.245.12	10.20.76.93	HTTP	544	HTTP/1.1 200 OK (text/html)
1928	16:40:52,027044	10.20.76.93	128.119.245.12	HTTP	498	GET /favicon.ico HTTP/1.1
1962	16:40:52,147082	128.119.245.12	10.20.76.93	HTTP	538	HTTP/1.1 404 Not Found (text/html)

Internet Protocol Version 4, Src: 10.20.76.93, Dst: 128.119.245.12	Transmission Control Protocol, Src Port: 50657, Dst Port: 80, Seq: 1, Ack: 1, Len: 483	Hypertext Transfer Protocol
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:135.0) Gecko/20100101 Firefox/135.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n Accept-Language: pt-PT,pt;q=0.8,en;q=0.5,en-US;q=0.3\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n Priority: u=0, i\r\n Authorization: Basic d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcms=\r\n \r\n [Response in frame: 1920] [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]		