

Desvendando o HTTP com Wireshark

Parte 2

A Interação HTTP GET Condicional/Resposta

Digite o URL no navegador `http://redes.sj.ifsc.edu.br`. Seu navegador deve exibir um arquivo em HTML muito simples com duas linhas. Responda às seguintes perguntas questões

No.	Time	Source	Destination	Protocol	Length	Info
66	7.266078813	192.168.0.4	191.36.8.36	HTTP	500	GET / HTTP/1.1
68	7.561395895	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
70	7.581660782	192.168.0.4	191.36.8.36	HTTP	449	GET /favicon.ico HTTP/1.1
71	7.599111390	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
84	12.860182845	192.168.0.4	191.36.8.36	HTTP	605	GET / HTTP/1.1
86	13.108221935	191.36.8.36	192.168.0.4	HTTP	270	HTTP/1.1 304 Not Modified

1. Inspeção o conteúdo da primeira mensagem - HTTP GET - do seu navegador para o servidor `redes.sj.ifsc.edu.br`. Você vê uma linha “If-Modified-Since”?

Não apareceu essa linha. O que significa que nessa primeira requisição ao servidor, o navegador não tem uma versão armazenada em cache ainda, então não fez uma verificação condicional.

2. Inspeção o conteúdo da resposta do servidor, segunda mensagem. O servidor retornou explicitamente o conteúdo do arquivo? Como você pode dizer isso?

Sim, pois está incluso o código HTTP/1.1 200 OK e também tem uma seção Content-Length de 1257 bytes, o que significa que o conteúdo foi enviado ao cliente.

No.	Time	Source	Destination	Protocol	Length	Info
66	7.266078813	192.168.0.4	191.36.8.36	HTTP	500	GET / HTTP/1.1
68	7.561395895	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
70	7.581660782	192.168.0.4	191.36.8.36	HTTP	449	GET /favicon.ico HTTP/1.1
71	7.599111390	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
84	12.860182845	192.168.0.4	191.36.8.36	HTTP	605	GET / HTTP/1.1
86	13.108221935	191.36.8.36	192.168.0.4	HTTP	270	HTTP/1.1 304 Not Modified

Frame 68: 406 bytes on wire (3248 bits), 406 bytes captured (3248 bits) on interface wlo1, Ethernet II, Src: SagemcomBroa_01:87:c5 (cc:58:30:01:87:c5), Dst: Intel_7d:3b:f1 (ec:63:d7:00:00:00), Internet Protocol Version 4, Src: 191.36.8.36, Dst: 192.168.0.4, Transmission Control Protocol, Src Port: 80, Dst Port: 49236, Seq: 1, Ack: 435, Len: 340	0000	ec 63 d7 7d 3b f1 cc 58 3
Hypertext Transfer Protocol	0010	01 88 a5 38 40 00 38 06 1
HTTP/1.1 200 OK\r\n	0020	00 04 00 50 c0 54 ed 9f e
Content-Type: text/html\r\n	0030	01 e6 eb 14 00 00 01 01 0
Accept-Ranges: bytes\r\n	0040	94 87 48 54 54 50 2f 31 2
ETag: "2422842869"\r\n	0050	4b 0d 0a 43 6f 6e 74 65 6
Last-Modified: Thu, 14 Mar 2024 18:00:21 GMT\r\n	0060	20 74 65 78 74 2f 68 74 6
Content-Length: 1257\r\n	0070	70 74 2d 52 61 6e 67 65 7
Date: Sat, 12 Oct 2024 18:45:25 GMT\r\n	0080	0d 0a 45 54 61 67 3a 20 2
	0090	38 36 39 22 0d 0a 4c 61 7
	00a0	69 65 64 3a 20 54 68 75 2
	00b0	20 32 20 22 34 20 31 38 2

3. Agora inspecione o conteúdo da terceira mensagem - HTTP GET - do seu navegador para o servidor. Você vê uma linha “If-Modified-Since”? Caso a resposta seja afirmativa, qual informação segue o cabeçalho “If-Modified-Since”?

Sim, apareceu o campo “If-Modified-Since”. A informação do cabeçalho é “Thu, 14 Mar 2024 18:00:21 GMT”

The image shows a Wireshark packet capture of an HTTP GET request and its response. The packet list on the left shows five packets. Packet 84 is the response, which is an HTTP 304 Not Modified. The packet details pane on the right shows the structure of the response, including the GET method, host, connection, cache-control, upgrade-insecure-requests, user-agent, accept, accept-encoding, accept-language, if-none-match, and if-modified-since headers.

No.	Time	Source	Destination	Protocol	Length	Info
66	7.266078813	192.168.0.4	191.36.8.36	HTTP	500	GET / HTTP/1.1
68	7.561395895	191.36.8.36	192.168.0.4	HTTP	406	HTTP/1.1 200 OK (text/html)
70	7.581660782	192.168.0.4	191.36.8.36	HTTP	449	GET /favicon.ico HTTP/1.1
71	7.599111390	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
84	12.860182845	192.168.0.4	191.36.8.36	HTTP	605	GET / HTTP/1.1
86	13.108221935	191.36.8.36	192.168.0.4	HTTP	270	HTTP/1.1 304 Not Modified

Frame 84: 605 bytes on wire (4840 bits), 605 bytes captured (4840 bits) on interface wlo1, Ethernet II, Src: Intel 7d:3b:f1 (ec:63:d7:7d:3b:f1), Dst: SagemcomBroa_01:87:c5 (cc:58:30:2e:69:66), Internet Protocol Version 4, Src: 192.168.0.4, Dst: 191.36.8.36, Transmission Control Protocol, Src Port: 49236, Dst Port: 80, Seq: 818, Ack: 1721, Len: 539, Hypertext Transfer Protocol

GET / HTTP/1.1\r\nHost: redes.sj.ifsc.edu.br\r\nConnection: keep-alive\r\nCache-Control: max-age=0\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/svg+xml\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9,pt;q=0.8\r\nIf-None-Match: "2422842869"\r\nIf-Modified-Since: Thu, 14 Mar 2024 18:00:21 GMT\r\n\r\n

4. Qual é o código de status e a frase retornada do servidor na resposta à terceira mensagem HTTP GET? É diferente do código de retorno da primeira mensagem? Qual é o código?

O código de status e a frase da terceira mensagem HTTP GET é “HTTP/1.1 304 Not Modified”. Já na primeira mensagem foi “HTTP/1.1 200 OK”. O que indica que o conteúdo não foi modificado desde a data que está no cabeçalho “If-Modified-Since”, então o servidor não precisa enviar o conteúdo novamente.

5. Na terceira resposta, o servidor retornou explicitamente o conteúdo do arquivo? Explique.

Na terceira resposta o servidor não retornou explicitamente o conteúdo, pois na primeira mensagem houve o retorno de 1257 bytes, já na terceira resposta houve o código 304 (não inclui o conteúdo do arquivo) e seu tamanho é reduzido para 270 bytes.

6. Qual o tamanho da primeira e terceira mensagem de retorno (respostas) do servidor?

A primeira mensagem é 1257 bytes e a terceira é 270 bytes.

Baixando Documentos Longos

(Foi aberto o URL “ http://redes.sj.ifsc.edu.br/Redes_arq2.htm” e atualizada a página uma vez)

1. Quantas mensagens HTTP GET foram enviadas pelo seu navegador? (desconsidere a requisição e resposta (erro) da mensagem favicon)

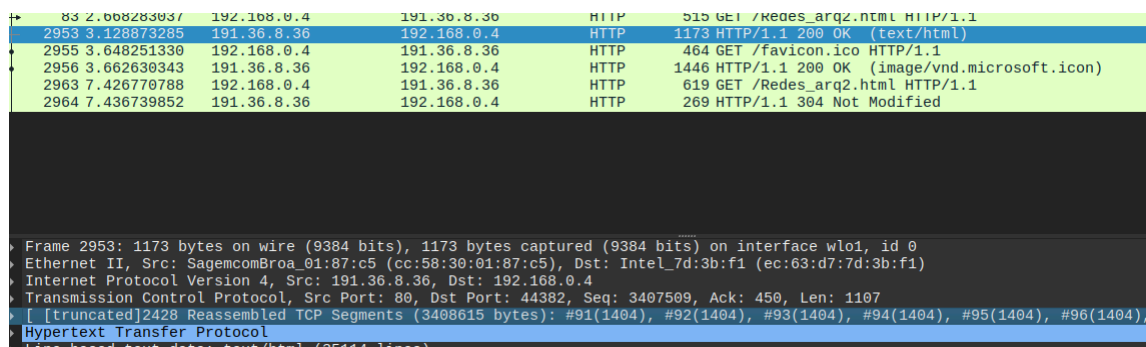
Duas mensagens HTTP GET, desconsiderando a requisição favicon.

2. Quantas respostas HTTP sua máquina recebeu?

Foram recebidas duas respostas HTTP, a primeira em relação à requisição “/Redes_arq2.html” e a outra ao refresh da página.

3. Quantos segmentos TCP foram necessários para carregar a resposta?

Foram necessários 2428 segmentos TCP.

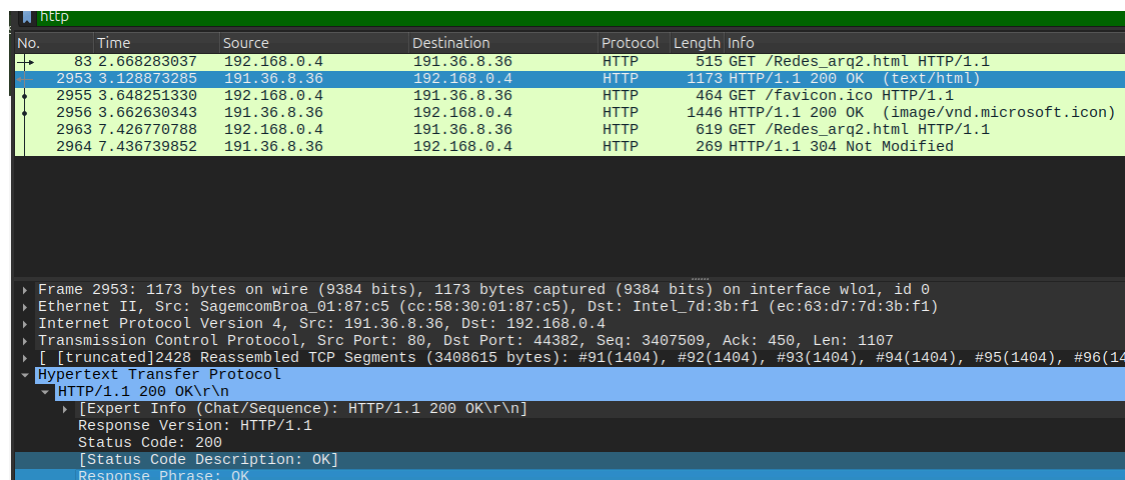


The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows several packets, with packet 2953 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 200 OK response. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
83	2.668283037	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq2.html HTTP/1.1
2953	3.128873285	191.36.8.36	192.168.0.4	HTTP	1173	HTTP/1.1 200 OK (text/html)
2955	3.648251330	192.168.0.4	191.36.8.36	HTTP	464	GET /favicon.ico HTTP/1.1
2956	3.662630343	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2963	7.426770788	192.168.0.4	191.36.8.36	HTTP	619	GET /Redes_arq2.html HTTP/1.1
2964	7.436739852	191.36.8.36	192.168.0.4	HTTP	269	HTTP/1.1 304 Not Modified

4. Qual é o código de status e a frase associada com a resposta à mensagem HTTP GET? Obs.: Observe os campos do cabeçalho de uma resposta HTTP.

O código de status e a frase associada é OK, o que significa que a requisição foi bem-sucedida.

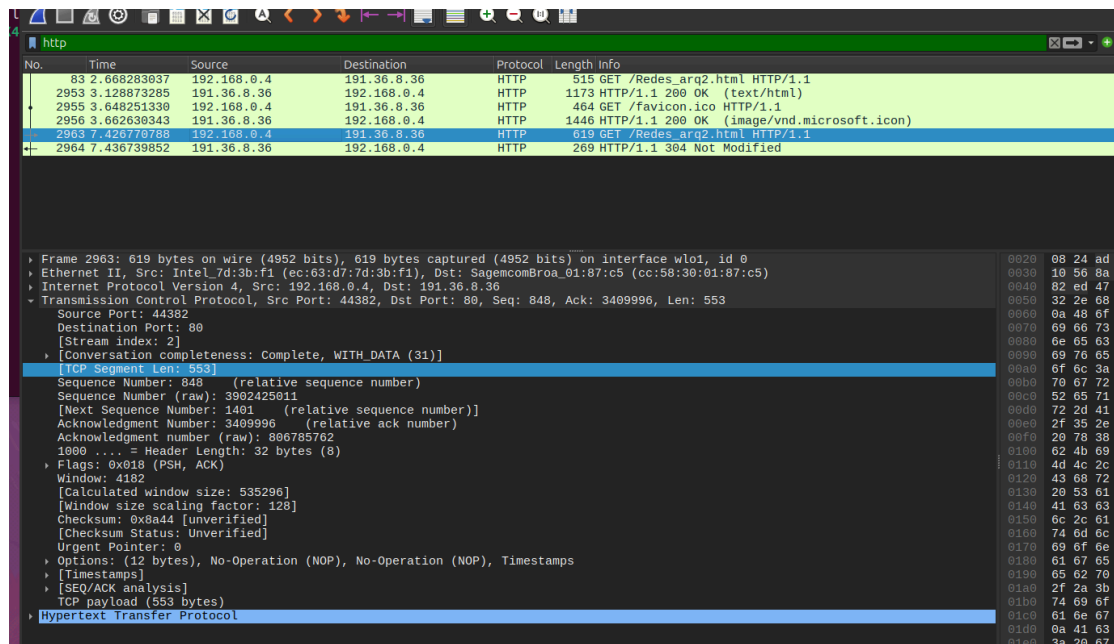


The image shows a Wireshark packet capture of an HTTP transaction. The packet list on the left shows several packets, with packet 2953 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 200 OK response. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
83	2.668283037	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq2.html HTTP/1.1
2953	3.128873285	191.36.8.36	192.168.0.4	HTTP	1173	HTTP/1.1 200 OK (text/html)
2955	3.648251330	192.168.0.4	191.36.8.36	HTTP	464	GET /favicon.ico HTTP/1.1
2956	3.662630343	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2963	7.426770788	192.168.0.4	191.36.8.36	HTTP	619	GET /Redes_arq2.html HTTP/1.1
2964	7.436739852	191.36.8.36	192.168.0.4	HTTP	269	HTTP/1.1 304 Not Modified

5. Quantos segmentos TCP foram necessários para obtenção da segunda resposta do servidor?

Um único segmento de 553 bytes.



No.	Time	Source	Destination	Protocol	Length	Info
83	2.668283037	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq2.html HTTP/1.1
2953	3.128873285	191.36.8.36	192.168.0.4	HTTP	1173	HTTP/1.1 200 OK (text/html)
2955	3.648251338	192.168.0.4	191.36.8.36	HTTP	464	GET /favicon.ico HTTP/1.1
2956	3.662630343	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
2963	7.426770788	192.168.0.4	191.36.8.36	HTTP	619	GET /Redes_arq2.html HTTP/1.1
2964	7.436739852	191.36.8.36	192.168.0.4	HTTP	269	HTTP/1.1 304 Not Modified

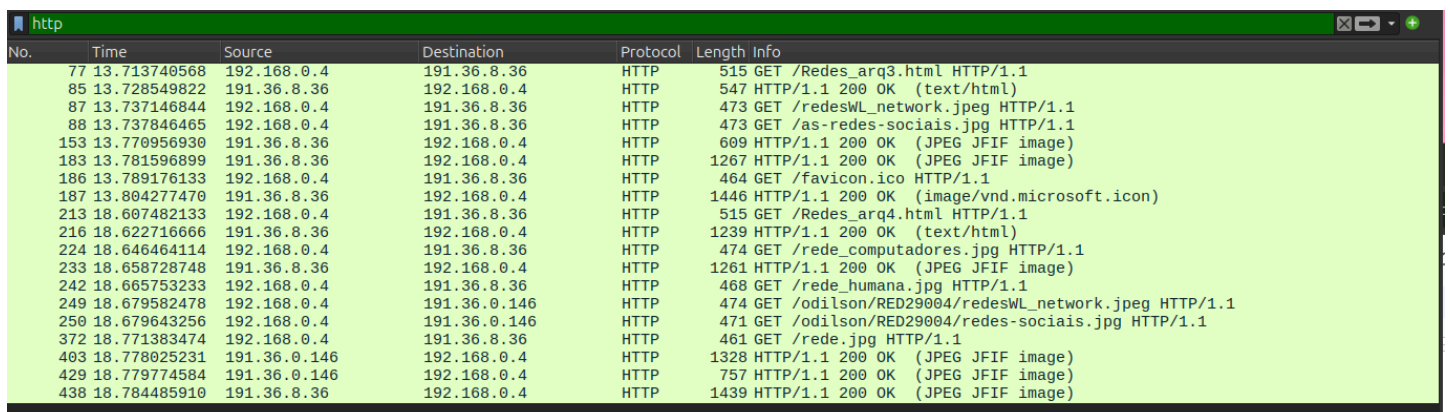
Frame 2963: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface wlo1, id 0
Ethernet II, Src: Intel_7d:3b:f1 (ec:63:d7:7d:3b:f1), Dst: SagemcomBroa_01:87:c5 (cc:58:30:01:87:c5)
Internet Protocol Version 4, Src: 192.168.0.4, Dst: 191.36.8.36
Transmission Control Protocol, Src Port: 44382, Dst Port: 80, Seq: 848, Ack: 3409996, Len: 553
Source Port: 44382
Destination Port: 80
[Stream index: 2]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 553]
Sequence Number: 848 (relative sequence number)
Sequence Number (raw): 3902425011
[Next Sequence Number: 1401 (relative sequence number)]
Acknowledgment Number: 3409996 (relative ack number)
Acknowledgment number (raw): 806785762
1000 = Header Length: 32 bytes (8)
Flags: 0x018 (PSH, ACK)
Window: 4182
[calculated window size: 535296]
[window size scaling factor: 128]
Checksum: 0x8a44 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (553 bytes)
Hypertext Transfer Protocol

6. O que explica a diferença entre a primeira e segunda requisições?

A segunda resposta tem um código 304 Not Modified, indicando que o conteúdo não foi modificado desde a última vez que foi requisitado, e por isso, não há envio de conteúdo adicional. Assim, na primeira requisição o arquivo completo foi baixado, já na segunda, esse processo todo não teve necessidade.

Documentos HTML com Objetos Incluídos

1.. Responda às seguintes questões, separando as respostas para o acesso ao Redes_arq3.html e Redes_arq4.html (6 respostas):



No.	Time	Source	Destination	Protocol	Length	Info
77	13.713740568	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq3.html HTTP/1.1
85	13.728549822	191.36.8.36	192.168.0.4	HTTP	547	HTTP/1.1 200 OK (text/html)
87	13.737146844	192.168.0.4	191.36.8.36	HTTP	473	GET /redesWL_network.jpeg HTTP/1.1
88	13.737846465	192.168.0.4	191.36.8.36	HTTP	473	GET /as-redes-sociais.jpg HTTP/1.1
153	13.770956930	191.36.8.36	192.168.0.4	HTTP	609	HTTP/1.1 200 OK (JPEG JFIF image)
183	13.781596899	191.36.8.36	192.168.0.4	HTTP	1267	HTTP/1.1 200 OK (JPEG JFIF image)
186	13.789176133	192.168.0.4	191.36.8.36	HTTP	464	GET /favicon.ico HTTP/1.1
187	13.804277470	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
213	18.607482133	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq4.html HTTP/1.1
216	18.622716666	191.36.8.36	192.168.0.4	HTTP	1239	HTTP/1.1 200 OK (text/html)
224	18.646464114	192.168.0.4	191.36.8.36	HTTP	474	GET /rede_computadores.jpg HTTP/1.1
233	18.658728748	191.36.8.36	192.168.0.4	HTTP	1261	HTTP/1.1 200 OK (JPEG JFIF image)
242	18.665753233	192.168.0.4	191.36.8.36	HTTP	468	GET /rede_humana.jpg HTTP/1.1
249	18.679582478	192.168.0.4	191.36.0.146	HTTP	474	GET /odilson/RED29004/redesWL_network.jpeg HTTP/1.1
250	18.679643256	192.168.0.4	191.36.0.146	HTTP	471	GET /odilson/RED29004/redes-sociais.jpg HTTP/1.1
372	18.771383474	192.168.0.4	191.36.8.36	HTTP	461	GET /rede.jpg HTTP/1.1
403	18.778025231	191.36.0.146	192.168.0.4	HTTP	1328	HTTP/1.1 200 OK (JPEG JFIF image)
429	18.779774584	191.36.0.146	192.168.0.4	HTTP	757	HTTP/1.1 200 OK (JPEG JFIF image)
438	18.784485910	191.36.8.36	192.168.0.4	HTTP	1439	HTTP/1.1 200 OK (JPEG JFIF image)

1.1. Quantas mensagens HTTP GET foram enviadas pelo seu navegador em cada acesso? (desconsidere a requisição e resposta (erro) da mensagem favicon)

- Redes_arq3_html

3 requisições HTTP GET: Uma para o próprio arquivo HTML e duas para cada uma das imagens referenciadas.

- Redes_arq4_html

6 requisições HTTP GET: Uma para o próprio arquivo HTML e cinco para cada uma das imagens referenciadas.

1.2. Para quais endereços na Internet (URI = Host + URL) estas mensagens foram enviadas em cada acesso?

- Redes_arq3_html

- Próprio HTML: “http://redes.sj.ifsc.edu.br/Redes_arq3.html”.
- Imagens: “http://redes.sj.ifsc.edu.br/redesWL_network.jpeg” e também “<http://redes.sj.ifsc.edu.br/as-redes-sociais.jpg>”.

- Redes_arq4_html

- Próprio HTML: “http://redes.sj.ifsc.edu.br/Redes_arq4.html”.
- Imagens: “http://redes.sj.ifsc.edu.br/rede_computadores.jpg”, “http://redes.sj.ifsc.edu.br/rede_humana.jpg”, “http://docente.ifsc.edu.br/odilson/RED29004/redesWL_network.jpeg”, “<http://docente.ifsc.edu.br/odilson/RED29004/redes-sociais.jpg>” e também “<http://redes.sj.ifsc.edu.br/rede.jpg>”.

1.3. Você consegue dizer se o seu navegador baixou imagens com ou sem paralelismo? Explique e diferencie o comportamento do navegador com e sem paralelismo.

- Redes_arq3_html

Com paralelismo.

- Redes_arq4_html

Com paralelismo.

No.	Time	Source	Destination	Protocol	Length	Info
77	13.713740568	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq3.html HTTP/1.1
85	13.728549822	191.36.8.36	192.168.0.4	HTTP	547	HTTP/1.1 200 OK (text/html)
87	13.737146844	192.168.0.4	191.36.8.36	HTTP	473	GET /redesWL_network.jpeg HTTP/1.1
88	13.737846465	192.168.0.4	191.36.8.36	HTTP	473	GET /as-redes-sociais.jpg HTTP/1.1
153	13.770956930	191.36.8.36	192.168.0.4	HTTP	609	HTTP/1.1 200 OK (JPEG JFIF image)
183	13.781596899	191.36.8.36	192.168.0.4	HTTP	1267	HTTP/1.1 200 OK (JPEG JFIF image)
186	13.789176133	192.168.0.4	191.36.8.36	HTTP	464	GET /favicon.ico HTTP/1.1
187	13.804277479	191.36.8.36	192.168.0.4	HTTP	1446	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
213	18.607482133	192.168.0.4	191.36.8.36	HTTP	515	GET /Redes_arq4.html HTTP/1.1
216	18.622716666	191.36.8.36	192.168.0.4	HTTP	1239	HTTP/1.1 200 OK (text/html)
224	18.646464114	192.168.0.4	191.36.8.36	HTTP	474	GET /rede_computadores.jpg HTTP/1.1
233	18.658728748	191.36.8.36	192.168.0.4	HTTP	1261	HTTP/1.1 200 OK (JPEG JFIF image)
242	18.665753233	192.168.0.4	191.36.8.36	HTTP	468	GET /rede_humana.jpg HTTP/1.1
249	18.679582473	192.168.0.4	191.36.0.146	HTTP	474	GET /odilson/RED29004/redesWL_network.jpeg HTTP/1.1
250	18.679643256	192.168.0.4	191.36.0.146	HTTP	471	GET /odilson/RED29004/redes-sociais.jpg HTTP/1.1
372	18.771383474	192.168.0.4	191.36.8.36	HTTP	461	GET /rede.jpg HTTP/1.1
403	18.778025231	191.36.0.146	192.168.0.4	HTTP	1328	HTTP/1.1 200 OK (JPEG JFIF image)
429	18.779774584	191.36.0.146	192.168.0.4	HTTP	757	HTTP/1.1 200 OK (JPEG JFIF image)
438	18.784485910	191.36.8.36	192.168.0.4	HTTP	1439	HTTP/1.1 200 OK (JPEG JFIF image)

Na imagem acima, as requisições HTTP indicam que várias imagens foram solicitadas com intervalos de tempo próximos, o que pode indicar o comportamento paralelo.

Com paralelismo, o navegador carrega vários recursos simultaneamente, e sem paralelismo, os recursos são baixados sequencialmente, resultando em um carregamento mais lento, o que resulta em um comportamento mais lento.