

Redes de Computadores

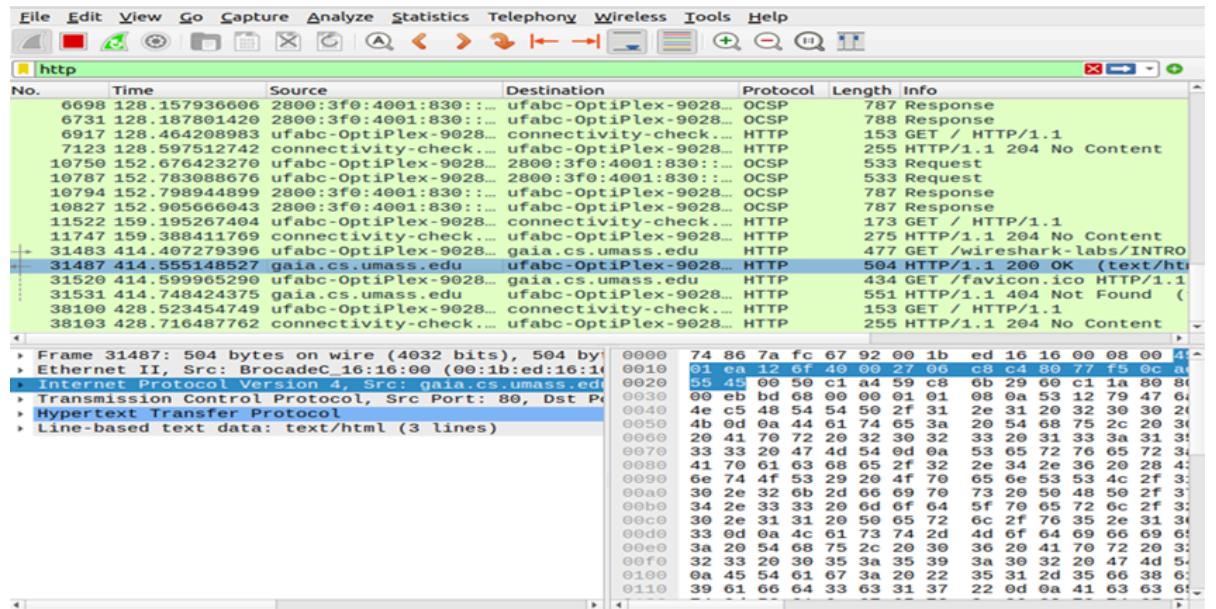
Náthaly Martins De Sá

Tópico 03

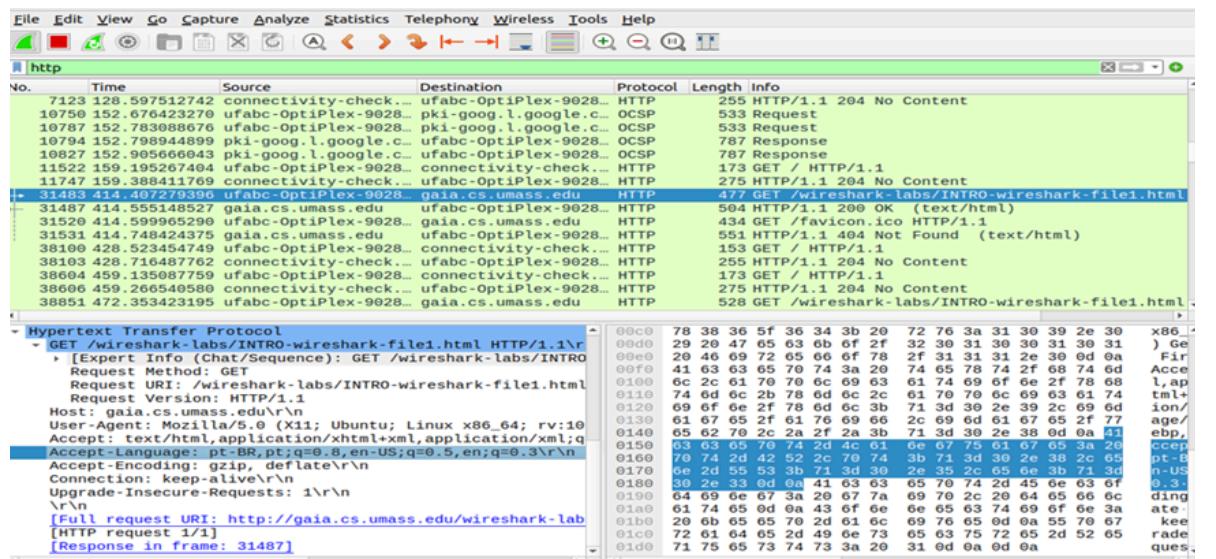
1. Interação básica HTTP.

1.1 Acesso: <http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html>

1.1.1 Versão do HTTP do navegador e do servidor web acessado:



1.1.2 Línguas que o navegador aceita:



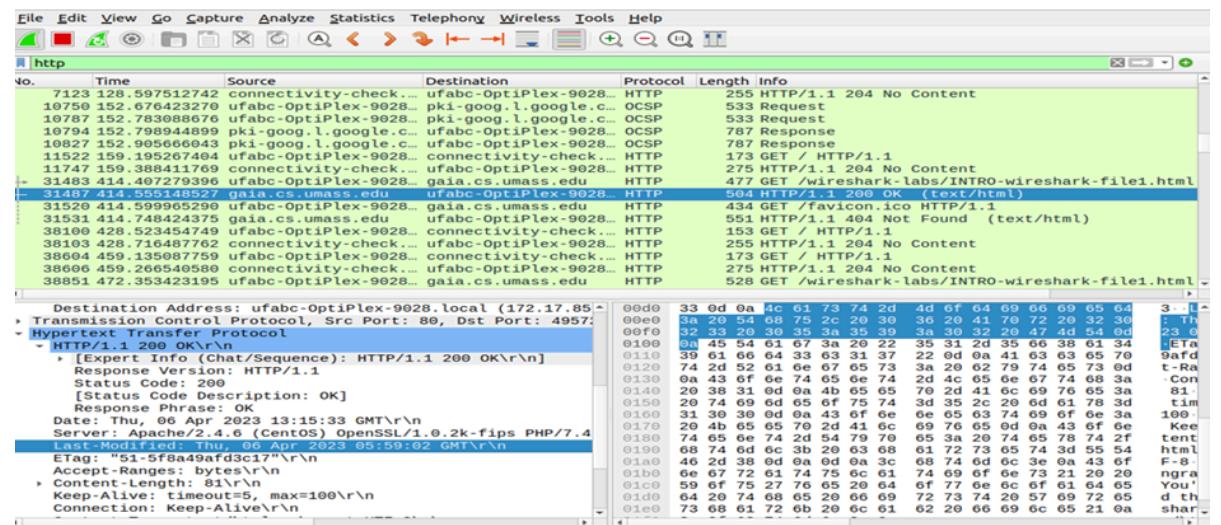
1.1.3 IP do seu computador e do servidor:

The screenshot shows a Wireshark interface with several network captures. The main pane displays a list of network frames, and the bottom pane shows the detailed content of frame 1. The status bar at the bottom indicates the date and time as Thu, 06 Apr 2023 13:15:33 GMT.

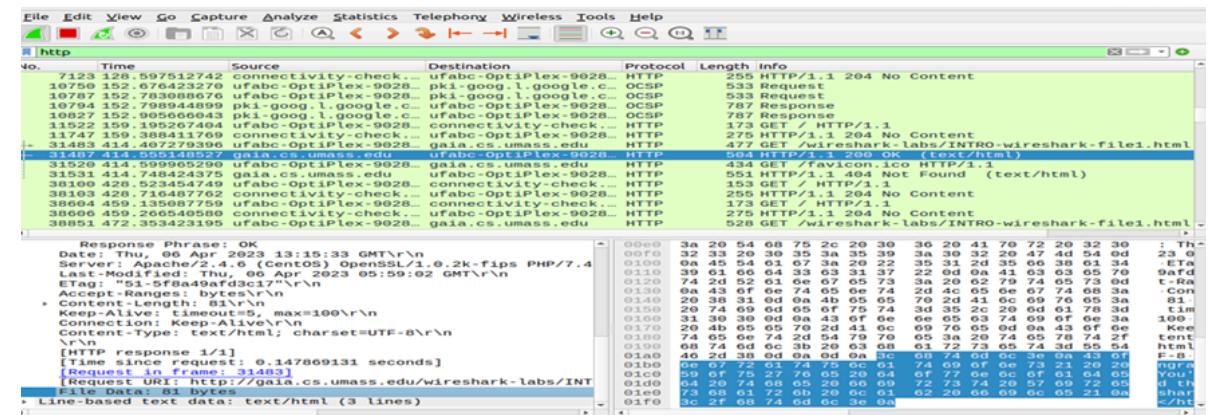
1.1.4 Código de status retornado do servidor para o navegador:

1.1.5 HTTP persistente ou não persistente:

1.1.6 Última modificação do arquivo HTML do servidor:



1.1.7 Número de bytes de conteúdo retornado ao navegador:



1.2 Análise os dados (raw data) do pacote:

É possível observar informações como as funcionalidades, número de quadros, desempenho, IP, flag, push, informações de janela deslizante e do cabeçalho TCP, entre outros.

2. GET Condisional.

2.1 Acesso: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html>

2.2 IF-MODIFIED-SINCE no HTTP GET:

The Wireshark interface shows a network capture. The selected frame (71038) is an HTTP GET request from the client 'ufabc-OptiPlex-9028' to the server 'gaia.cs.umass.edu'. The request includes the header 'If-Modified-Since: Thu, 06 Apr 2023 05:59:02 GMT'. The server responds with an HTTP 304 Not Modified message. The packet details pane shows the full request and response headers.

Logo, é sim possível observar ‘IF-MODIFIED-SINCE’.

2.3 Conteúdo do arquivo:

The Wireshark interface shows a network capture. The selected frame (80015) is an HTTP GET request from the client 'ufabc-OptiPlex-9028' to the server 'cslash.net' for the file '/E8_cover_small.jpg'. The server responds with an HTTP 200 OK message, indicating the file content is being sent. The packet details pane shows the full request and response headers, and the bytes pane shows the actual JPEG file content.

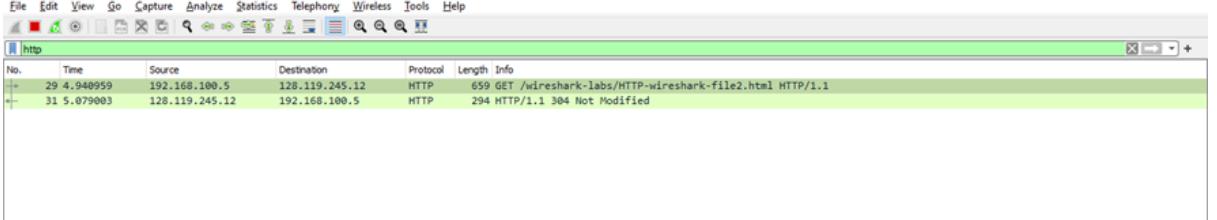
Logo, como observado acima, o servidor retorna o conteúdo do arquivo (arquivo JPEG).

2.4 IF-MODIFIED-SINCE no HTTP GET:

Ao examinar uma nova resposta do servidor no Wireshark, o campo IF-MODIFIED-SINCE continuará presente no cabeçalho HTTP como já apresentado (Item 2.2). Esse cabeçalho é utilizado pelo cliente para informar ao servidor a data e hora da última vez em que o cliente recebeu uma cópia

do recurso solicitado (além também de apresentar código de status, versão do protocolo, etc). O servidor pode então usar as informações para decidir se enviará novamente o conteúdo completo do recurso ou enviará apenas um código de status 304 (Not Modified), indicando que o recurso não foi modificado desde a última vez que o cliente o acessou.

2.5 Conteúdo do arquivo:



```

No. Time Source Destination Protocol Length Info
29 4.940959 192.168.100.5 128.119.245.12 HTTP 659 GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1
31 5.079003 128.119.245.12 192.168.100.5 HTTP 294 HTTP/1.1 304 Not Modified

```

> Frame 29: 659 bytes on wire (5272 bits), 659 bytes captured (5272 bits) on interface \Device\WPF_{C64418FC-C2F8-43FB-AFE9-E8FFCE47A630}, id 0
> Ethernet II, Src: Palladiu_00:ff:9c (Sc:c9:d3:60:7f:9c), Dst: HuaweiTe_9b:2f:ac (9c:74:1a:9b:2f:ac)
> Internet Protocol Version 4, Src: 192.168.100.5, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 51551, Dst Port: 80, Seq: 1, Ack: 1, Len: 605
< Hypertext Transfer Protocol
 < GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-wireshark-file2.html HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /wireshark-labs/HTTP-wireshark-file2.html
 Request Version: HTTP/1.1
 Host: gaia.cs.umass.edu\r\n
 Connection: keep-alive\r\n
 Cache-Control: max-age=0\r\n
 Upgrade-Insecure-Requests: 1\r\n
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
 Accept-Encoding: gzip, deflate\r\n
 Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7\r\n
 If-None-Match: "173-5f981e333adcb"\r\n
 If-Modified-Since: Mon, 17 Apr 2023 05:59:01 GMT\r\n
 \r\n
 [Full request URI: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file2.html]
 [HTTP request 1/1]
 [Response in frame: 31]

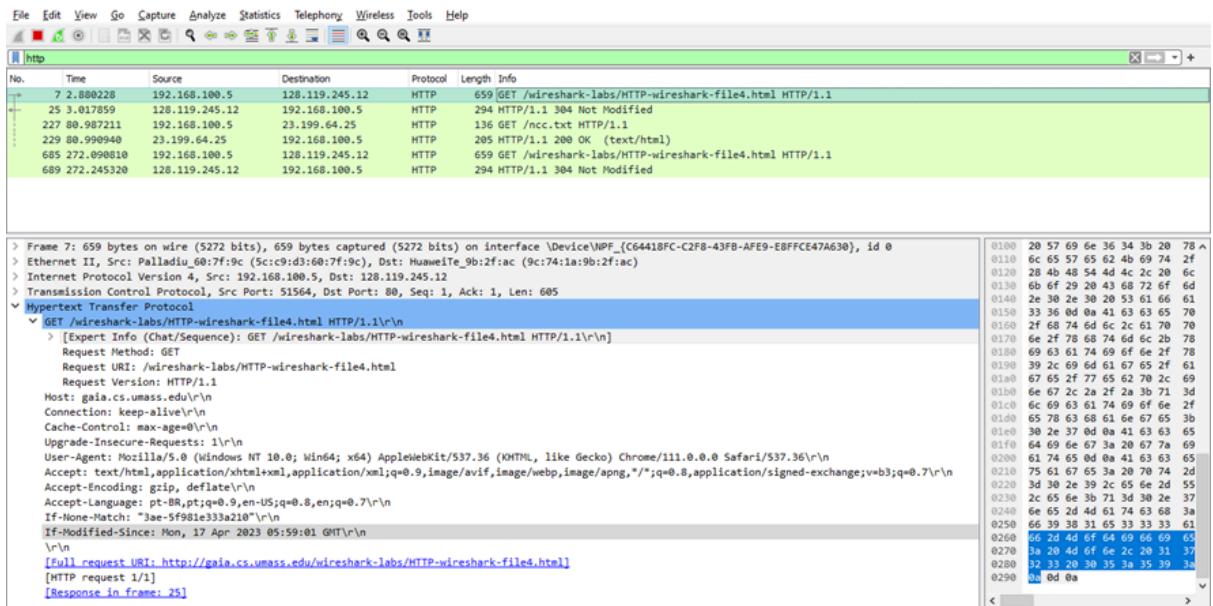
0100 20 57 69 6e 36 34 3b 2b 78 78
0110 6c 65 57 65 62 4b 69 74 2f
0120 28 4b 48 54 4d 4c 2c 2b 6c
0130 6b 6f 29 20 43 68 72 6f 6d
0140 2e 30 2e 30 20 53 61 66 61
0150 33 36 0d 0a 41 63 63 65 70
0160 2f 68 74 6d 6c 2c 61 70 70
0170 6e 2f 78 68 74 6d 6c 2b 78
0180 69 63 61 74 69 6f 6e 2f 78
0190 39 2c 69 6d 61 67 65 2f 61
01a0 67 65 2f 77 65 62 70 2c 69
01b0 6e 67 2c 2a 2f 2a 3b 71 3d
01c0 6c 69 63 61 74 69 6f 6e 2f
01d0 65 78 63 68 61 6e 67 65 3b
01e0 30 2b 57 0d 0a 41 63 63 65
01f0 61 74 69 6f 6e 2b 70 74 6d
0200 63 74 69 6f 6e 2f 70 74 6d
0210 75 61 67 65 3a 29 70 24 2d
0220 3d 30 2e 39 2c 2b 65 6e 2d 55
0230 2c 65 6e 2b 71 3d 30 2e 37
0240 6e 65 2d 4d 61 74 63 68 3a
0250 66 39 38 31 65 33 33 33 61
0260 66 2d 4d 6f 64 69 66 69 65
0270 3a 2b 4d 6f 6e 2c 20 31 37
0280 32 33 20 30 35 3a 25 39 3a
0290 0a 0d 0a

Agora ao verificar essa nova resposta do servidor, a saída se dá como NOT MODIFIED, isso porque a resposta do servidor para a segunda requisição GET pode ou não incluir o conteúdo completo do arquivo como citado no item acima, dependendo do conteúdo do cabeçalho HTTP enviado pelo cliente e das informações armazenadas pelo servidor sobre o recurso.

3. HTML com objetos.

3.1 Acesso: <http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file4.html>

3.2 Número de requisições HTTP GET e endereço IP:



Foram realizadas 3 requisições HTTP feitas pelo navegador para o endereço IP 128.119.245.12.

3.3 Download das imagens (objetos):

O download dos objetos foi feito de maneira paralela, pois as portas eram distintas. Como observável no item anterior, a página contém um total de 4 objetos (objetos 1 e 2 se tratam de imagens JPEG e os objetos 3 e 4 se tratam de arquivos HTML).

4. Autenticação HTTP.

4.1 Acesso:

<http://gaia.cs.umass.edu/wireshark-labs/protected-pages/HTTP-wireshark-file5.htm>

4.2 Resposta do servidor ao HTTP GET inicial do navegador:

The Wireshark interface displays a list of network frames. Frame 91405 shows an HTTP 1.1 401 Unauthorized response from the server. The details pane shows the response content, including the status code, reason phrase, and various headers like Date, Server, WWW-Authenticate, Content-Length, Keep-Alive, and Connection.

```

Frame 91405: 783 bytes on wire (6264 bits), 783 bytes captured
Ethernet II, Src: BrocadeC_18:aa:00 (00:1b:ed:18:aa:00), Dst: gaia.cs.umass.edu (128.119.245.12)
Internet Protocol Version 4, Src: gaia.cs.umass.edu (128.119.245.12), Dst: 0.0.0.0
Transmission Control Protocol, Src Port: 80, Dst Port: 50614
HTTP/1.1 401 Unauthorized\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized]
  Response Version: HTTP/1.1
  Status Code: 401
  [Status Code Description: Unauthorized]
  Response Phrase: Unauthorized
  Date: Thu, 06 Apr 2023 14:10:45 GMT\r\n
  Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.4
  WWW-Authenticate: Basic realm="wireshark-students only"\r\n
  Content-Length: 381\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n

```

Primeira informação disponibilizada é de que a página é protegida, logo no primeiro GET teremos acesso não autorizado, porém após feito o login, as informações da página aparecem nos GETs posteriores.

4.3 Campo incluído na segunda mensagem GET:

The Wireshark interface displays a list of network frames. Frame 138 shows an HTTP GET request with an Authorization header containing basic authentication credentials. The details pane shows the full request message, including the method, URL, headers (Host, Connection, Cache-Control, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language), and the full request URI.

```

Frame 138: 627 bytes on wire (5016 bits), 627 bytes captured (5016 bits) on interface \Device\NPF_{C64418FC-C2FB-43FB-AFE9-E8FFCE47A630}, id 0
Ethernet II, Src: Palladiu_60:7f:9c (5c:ch:d3:60:7f:9c), Dst: HuaweiTe_9b:2f:ac (9c:74:1a:9b:2f:ac)
Internet Protocol Version 4, Src: 192.168.100.5, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 51650, Dst Port: 80, Seq: 1, Ack: 1, Len: 573
HTTP/1.1 200 OK (text/html)
[full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 141]

GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /wireshark-labs/protected_pages/HTTP-wireshark-file5.html HTTP/1.1\r\n]
Request Method: GET
Request URL: /wireshark-labs/protected_pages/HTTP-wireshark-file5.html
Request Version: HTTP/1.1
Host: gaia.cs.umass.edu\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic d2lyZm9vYXJrLXN0dmlRbzOm5ldHdvcmw=\r\n
  Credentials: wireshark-students@network
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: pt-BR,pt;q=0.9\r\n
\r\n
[full request URI: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html]
[HTTP request 1/1]
[Response in frame: 141]

```

4.4 Segurança da autenticação HTTP:

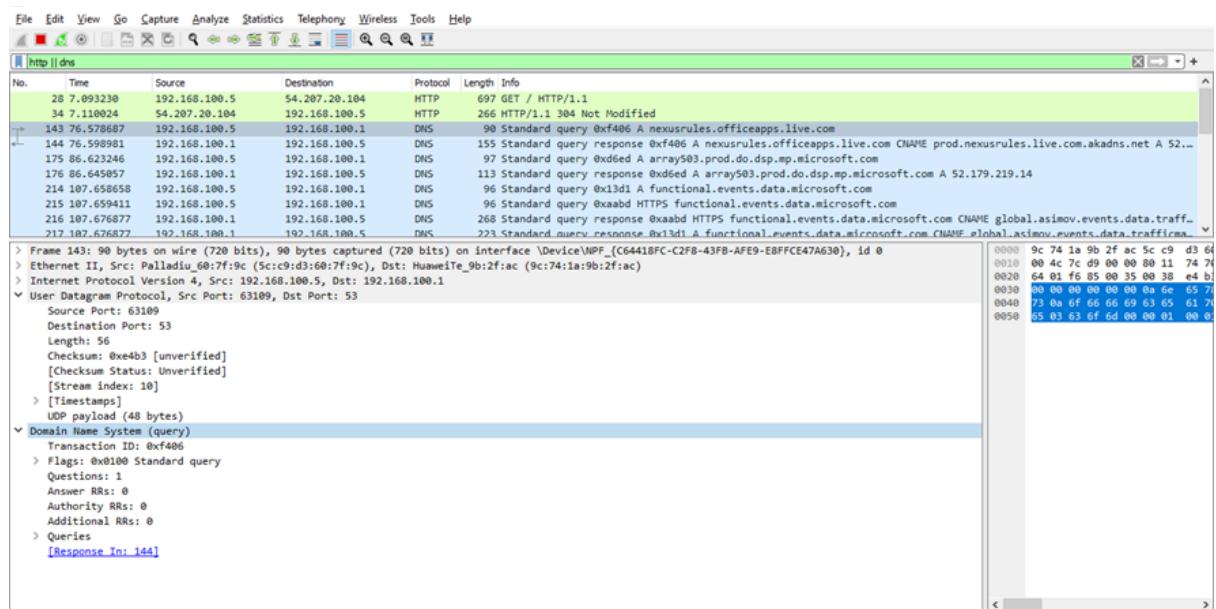
Sim, é possível visualizar o nome de usuário e senha na captura de pacotes, porém se encontram codificados em base64. Logo a autenticação HTTP não é um protocolo seguro, pois além de não fornecer nenhum mecanismo de segurança integrado para autenticação ou confidencialidade dos dados transmitidos, ainda é de fácil acesso a decodificação já que o nome de usuário e senha são enviados em texto simples (ainda que codificados em base64).

5. Resolução de nomes.

5.1 Acesso: ‘Pudim’;

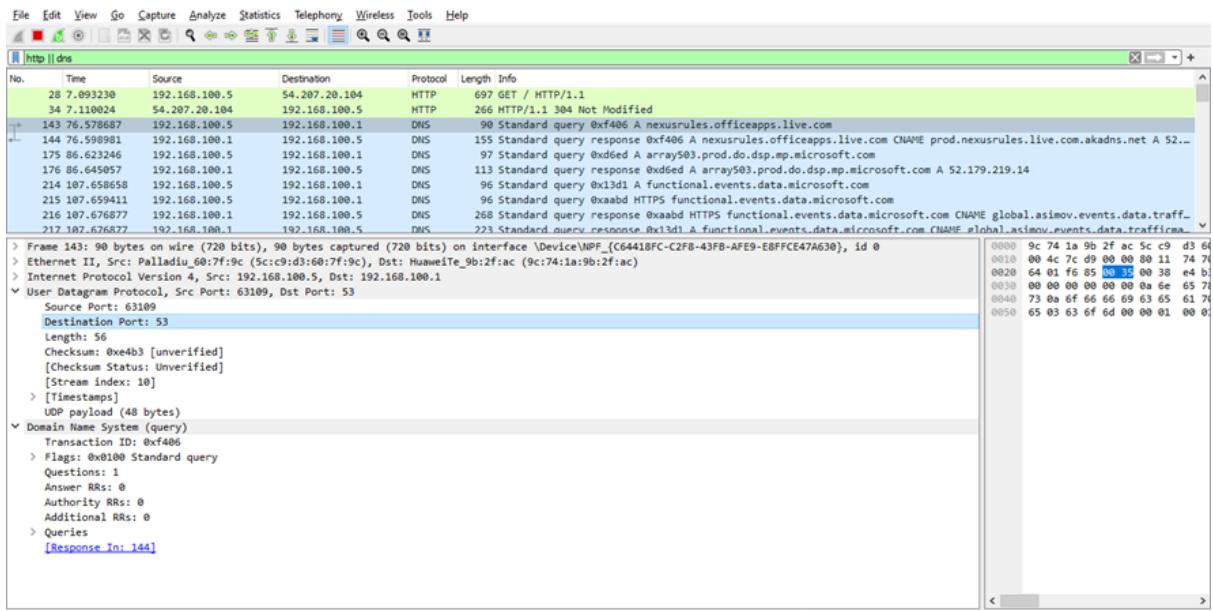
Filtro: DNS.

5.2 TCP ou UDP:



Como observável os pacotes DNS são enviados utilizando o protocolo UDP, logo se trata de um processo rápido, porém não seguro.

5.3 Porta de origem e porta de destino:



É possível observar que a mensagem query DNS é enviada para o servidor DNS na porta de destino 53 (DNS). Em seguida, o servidor DNS envia uma mensagem de resposta para o cliente na porta de origem aleatória que foi usada na mensagem query DNS.

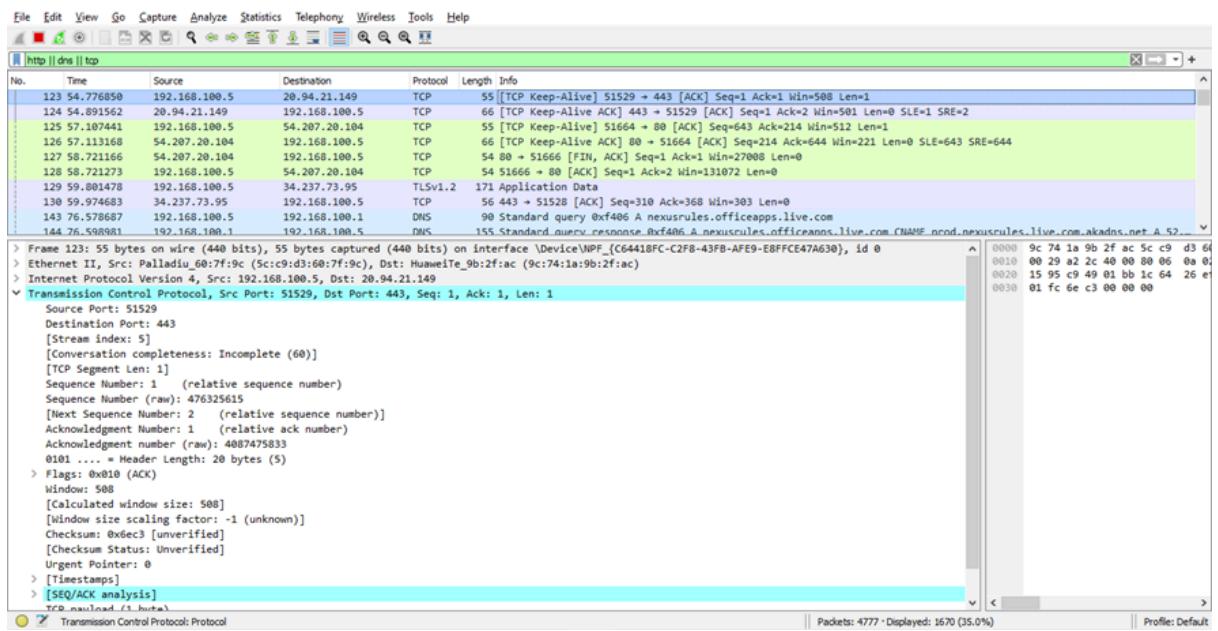
5.4 Endereço IP:

A mensagem de query do DNS foi enviada para um servidor DNS cujo endereço IP é 192.168.0.1. Esse endereço IP pode variar dependendo da configuração de rede do usuário, mas é comum que o roteador seja utilizado como servidor DNS padrão.

5.5 Respostas e seus conteúdos:

É apresentado apenas uma resposta do DNS, sendo seu conteúdo o endereço IP do servidor web 'Pudim'.

5.6 IP's:



Ao aplicar um filtro para visualizar apenas os pacotes TCP SYN enviados pelo navegador para o endereço de destino correspondente ao site do Pudim (52.84.246.89), podemos observar que sim, o IP de destino do pacote TCP SYN corresponde ao endereço IP fornecido pela mensagem de resposta DNS. Isso indica que o navegador está tentando estabelecer uma conexão TCP com o servidor web do Pudim para carregar o conteúdo do site.

5.7 Host e novas queries DNS:

Ao solicitar as imagens individualmente ao servidor, é feito uma única consulta DNS para obter o endereço IP do servidor que hospeda a página, sendo assim não é necessário fazer novas consultas DNS para cada imagem. O navegador utiliza o endereço IP armazenado em cache para se conectar diretamente ao servidor e solicitar cada imagem.