

UNIVERSIDADE FEDERAL DE ALAGOAS
CIÊNCIA DA COMPUTAÇÃO
REDES DE COMPUTADORES - 2022.2
NAYSE DA SILVA FAGUNDES

Trabalho 1 - Análise de Requisições HTTP

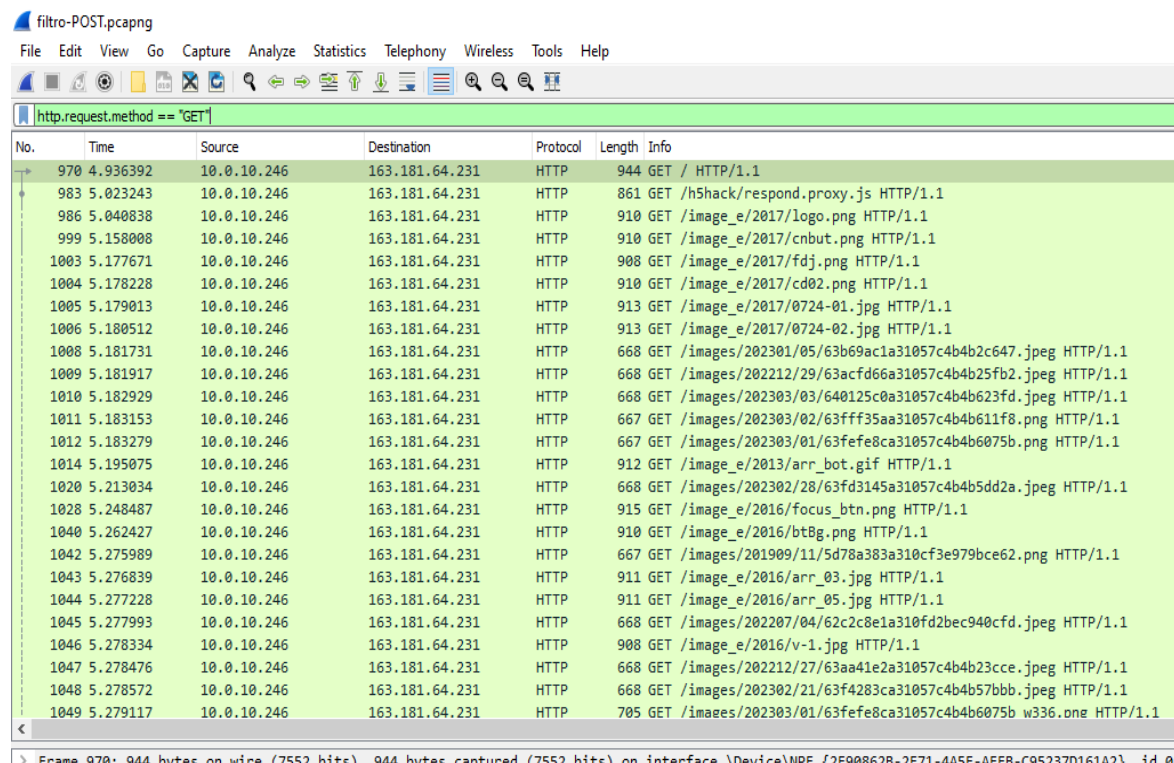
Download da aplicação Wireshark: [Wireshark · Go Deep](#)

Site utilizado para as requisições: **chinadaily.com.cn**

1. Ativar o Wireshark para monitorar a placa de rede em questão; **OK**.
2. Realizar uma requisição HTTP GET utilizando um cliente que desejar (ex.: browser Web, curl etc.) para alguma URL (na aula ao vivo, mostro como fazer isso pelo browser).

Para visualizar as requisições HTTP, é necessário abrir o Wireshark e depois iniciar a captura. Em seguida, utilizar os seguintes filtros:

http.request.method == "GET" - filtro para obter as solicitações HTTP que possuam o método GET

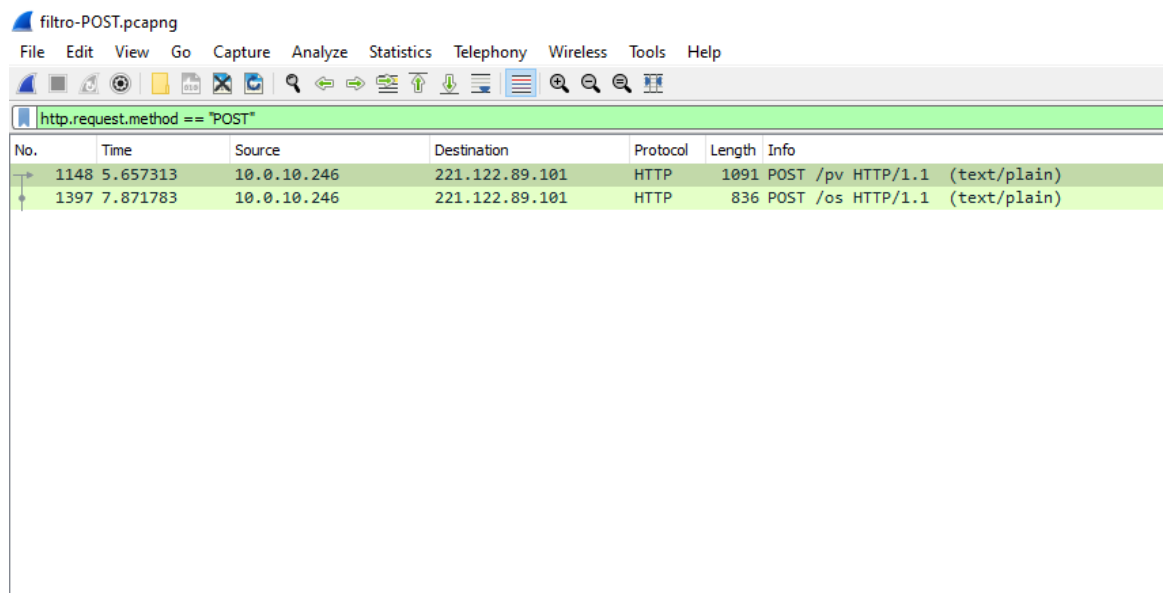


The screenshot shows the Wireshark network protocol analyzer interface. The filter bar at the top contains the filter `http.request.method == "GET"`. The packet list pane displays a series of HTTP GET requests from source IP 10.0.10.246 to destination IP 163.181.64.231. The selected packet (No. 970) is highlighted in green. The packet details pane shows the structure of the selected HTTP GET request.

No.	Time	Source	Destination	Protocol	Length	Info
970	4.936392	10.0.10.246	163.181.64.231	HTTP	944	GET / HTTP/1.1
983	5.023243	10.0.10.246	163.181.64.231	HTTP	861	GET /h5hack/respond.proxy.js HTTP/1.1
986	5.040838	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/logo.png HTTP/1.1
999	5.158008	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/cnbut.png HTTP/1.1
1003	5.177671	10.0.10.246	163.181.64.231	HTTP	908	GET /image_e/2017/fdj.png HTTP/1.1
1004	5.178228	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/cd02.png HTTP/1.1
1005	5.179013	10.0.10.246	163.181.64.231	HTTP	913	GET /image_e/2017/0724-01.jpg HTTP/1.1
1006	5.180512	10.0.10.246	163.181.64.231	HTTP	913	GET /image_e/2017/0724-02.jpg HTTP/1.1
1008	5.181731	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202301/05/63b69ac1a31057c4b4b2c647.jpeg HTTP/1.1
1009	5.181917	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202212/29/63acfd66a31057c4b4b25fb2.jpeg HTTP/1.1
1010	5.182929	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202303/03/640125c0a31057c4b4b623fd.jpeg HTTP/1.1
1011	5.183153	10.0.10.246	163.181.64.231	HTTP	667	GET /images/202303/02/63fff35aa31057c4b4b611f8.png HTTP/1.1
1012	5.183279	10.0.10.246	163.181.64.231	HTTP	667	GET /images/202303/01/63fefe8ca31057c4b4b6075b.png HTTP/1.1
1014	5.195075	10.0.10.246	163.181.64.231	HTTP	912	GET /image_e/2013/arr_bot.gif HTTP/1.1
1020	5.213034	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202302/28/63fd3145a31057c4b4b5dd2a.jpeg HTTP/1.1
1028	5.248487	10.0.10.246	163.181.64.231	HTTP	915	GET /image_e/2016/focus_btn.png HTTP/1.1
1040	5.262427	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2016/bt8g.png HTTP/1.1
1042	5.275989	10.0.10.246	163.181.64.231	HTTP	667	GET /images/201909/11/5d78a383a310cf3e979bce62.png HTTP/1.1
1043	5.276839	10.0.10.246	163.181.64.231	HTTP	911	GET /image_e/2016/arr_03.jpg HTTP/1.1
1044	5.277228	10.0.10.246	163.181.64.231	HTTP	911	GET /image_e/2016/arr_05.jpg HTTP/1.1
1045	5.277993	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202207/04/62c2c8e1a310fd2bec940cfd.jpeg HTTP/1.1
1046	5.278334	10.0.10.246	163.181.64.231	HTTP	908	GET /image_e/2016/v-1.jpg HTTP/1.1
1047	5.278476	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202212/27/63aa41e2a31057c4b4b23cce.jpeg HTTP/1.1
1048	5.278572	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202302/21/63f4283ca31057c4b4b57bbb.jpeg HTTP/1.1
1049	5.279117	10.0.10.246	163.181.64.231	HTTP	705	GET /images/202303/01/63fefe8ca31057c4b4b6075b_w336.png HTTP/1.1

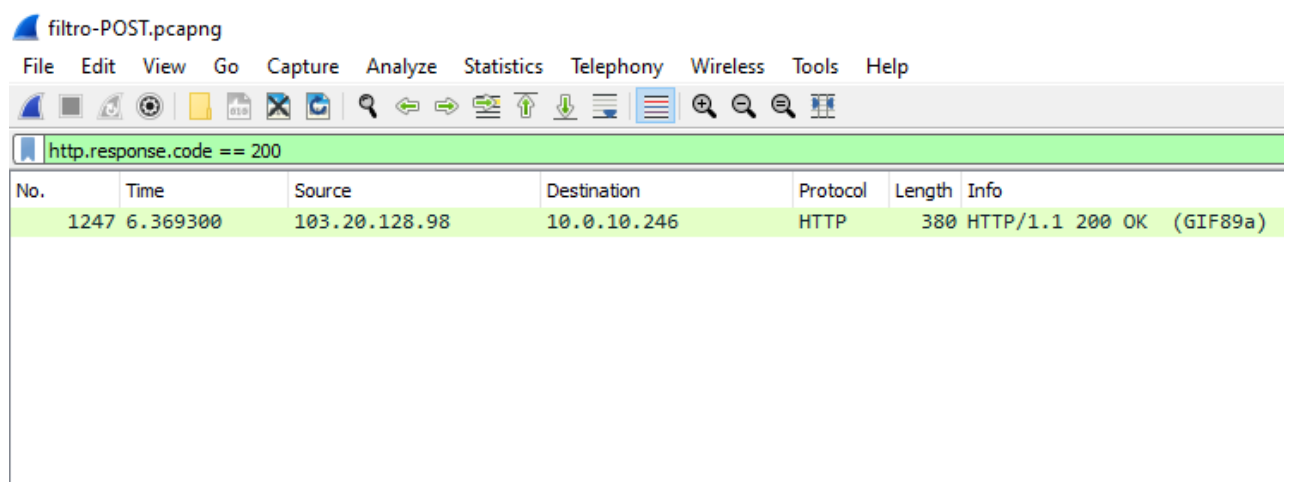
> Frame 970: 944 bytes on wire (7552 bits). 944 bytes captured (7552 bits) on interface \Device\NPF {2F90862B-2F71-4A5F-AFFB-C95237D161A2}. id 0

http.request.method == "POST" filtro para obter as solicitações HTTP que possuam o método POST



3. Utilizando o Wireshark, filtrar os principais parâmetros da requisição e de resposta HTTP GET.
Ex.: Status, código de resposta, se usa ou não cookie, se usa HTTP GET CONDICIONAL etc.

Status e Código de resposta: Utilizando o filtro de código de resposta: **http.response.code == 200**, para verificar se a solicitação foi bem sucedida:



filtro-POST.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 404

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

filtro-POST.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.response.code == 500

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Utiliza cookies: SIM, é possível verificar utilizando o filtro **http.cookie**:

Em seguida é possível visualizar que em algumas das solicitações HTTP que existe os termos cookies e set-cookie no cabeçalho da solicitação:

filtro-POST.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.cookie

No.	Time	Source	Destination	Protocol	Length	Info
970	4.936392	10.0.10.246	163.181.64.231	HTTP	944	GET / HTTP/1.1
983	5.023243	10.0.10.246	163.181.64.231	HTTP	861	GET /h5hack/respond.proxy.js HTTP/1.1
986	5.040838	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/logo.png HTTP/1.1
999	5.158008	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/cnbut.png HTTP/1.1
1003	5.177671	10.0.10.246	163.181.64.231	HTTP	908	GET /image_e/2017/fdj.png HTTP/1.1
1004	5.178228	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2017/cd02.png HTTP/1.1
1005	5.179013	10.0.10.246	163.181.64.231	HTTP	913	GET /image_e/2017/0724-01.jpg HTTP/1.1
1006	5.180512	10.0.10.246	163.181.64.231	HTTP	913	GET /image_e/2017/0724-02.jpg HTTP/1.1
1008	5.181731	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202301/05/63b69ac1a31057c4b4b2c647.jpeg HTTP/1.1
1009	5.181917	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202212/29/63acfd66a31057c4b4b25fb2.jpeg HTTP/1.1
1010	5.182929	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202303/03/640125c0a31057c4b4b623fd.jpeg HTTP/1.1
1011	5.183153	10.0.10.246	163.181.64.231	HTTP	667	GET /images/202303/02/63fff35aa31057c4b4b611f8.png HTTP/1.1
1012	5.183279	10.0.10.246	163.181.64.231	HTTP	667	GET /images/202303/01/63fefe8ca31057c4b4b6075b.png HTTP/1.1
1014	5.195075	10.0.10.246	163.181.64.231	HTTP	912	GET /image_e/2013/arr_bot.gif HTTP/1.1
1020	5.213034	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202302/28/63fd3145a31057c4b4b5dd2a.jpeg HTTP/1.1
1028	5.248487	10.0.10.246	163.181.64.231	HTTP	915	GET /image_e/2016/focus_btn.png HTTP/1.1
1040	5.262427	10.0.10.246	163.181.64.231	HTTP	910	GET /image_e/2016/bt0g.png HTTP/1.1
1042	5.275989	10.0.10.246	163.181.64.231	HTTP	667	GET /images/201909/11/5d78a383a310cf3e979bce62.png HTTP/1.1
1043	5.276839	10.0.10.246	163.181.64.231	HTTP	911	GET /image_e/2016/arr_03.jpg HTTP/1.1
1044	5.277228	10.0.10.246	163.181.64.231	HTTP	911	GET /image_e/2016/arr_05.jpg HTTP/1.1
1045	5.277993	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202207/04/62c2c8e1a310fd2bec940cfd.jpeg HTTP/1.1
1046	5.278334	10.0.10.246	163.181.64.231	HTTP	908	GET /image_e/2016/v-1.jpg HTTP/1.1
1047	5.278476	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202212/27/63aa41e2a31057c4b4b23cce.jpeg HTTP/1.1
1048	5.278572	10.0.10.246	163.181.64.231	HTTP	668	GET /images/202302/21/63f4283ca31057c4b4b57bbb.jpeg HTTP/1.1
1049	5.279117	10.0.10.246	163.181.64.231	HTTP	705	GET /images/202303/01/63fefe8ca31057c4b4b6075b_w336.png HTTP/1.1

HTTP GET CONDICIONAL: SIM, existe no cabeçalho de alguns GET o termo If-Modified-Since:

```
<
> Frame 1049: 705 bytes on wire (5640 bits), 705 bytes captured (5640 bits) on interface \Device\NPF_{2E90862B-2F71-4A5E-AEFB-C95237D161A2}, id 0
> Ethernet II, Src: 9a:83:f6:db:48:3b (9a:83:f6:db:48:3b), Dst: TP-Link_bb:b4:bc (00:5f:67:bb:b4:bc)
> Internet Protocol Version 4, Src: 10.0.10.246, Dst: 163.181.64.231
> Transmission Control Protocol, Src Port: 49838, Dst Port: 80, Seq: 615, Ack: 518, Len: 651
✓ Hypertext Transfer Protocol
  > GET /images/202303/01/63fefe8ca31057c4b4b6075b_w336.png HTTP/1.1\r\n
    Host: img2.chinadaily.com.cn\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Wed, 01 Mar 2023 07:28:12 GMT\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 Edg/111.0.1661.44\r\n
    If-None-Match: "63fefe8c-2182d"\r\n
    Accept: image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8\r\n
    Referer: http://www.chinadaily.com.cn/\r\n
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: pt-BR,pt;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
  > Cookie: __asc=52b471241870c0fec74673f0f72; __auc=52b471241870c0fec74673f0f72; wdcid=77b9118484be3d00\r\n
    \r\n
    [Full request URI: http://img2.chinadaily.com.cn/images/202303/01/63fefe8ca31057c4b4b6075b_w336.png]
    [HTTP request 2/4]
    [Prev request in frame: 1020]
    [Response in frame: 1068]
    [Next request in frame: 1092]
```

Frame 970: 944 bytes on wire (7552 bits), 944 bytes captured (7552 bits) on interface
\\Device\NPF_{2E90862B-2F71-4A5E-AEFB-C95237D161A2}, id 0
Ethernet II, Src: 9a:83:f6:db:48:3b (9a:83:f6:db:48:3b), Dst: TP-Link_bb:b4:bc
(00:5f:67:bb:b4:bc)
Internet Protocol Version 4, Src: 10.0.10.246, Dst: 163.181.64.231
Transmission Control Protocol, Src Port: 49833, Dst Port: 80, Seq: 1, Ack: 1, Len: 890
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.chinadaily.com.cn\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 Edg/111.0.1661.44\r\n
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,appli
cation/signed-exchange;v=b3;q=0.7\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: pt-BR,pt;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
[truncated]Cookie: __asc=52b471241870c0fec74673f0f72;
__auc=52b471241870c0fec74673f0f72; wdcid=77b9118484be3d00;
wdses=206f59211b50533f; wdlast=1679535891; pt_s_3bfec6ad=vt=1679535893036&cad=;
pt_3bfec6ad=uid=iNDlgpzvZLNfSpmB-S-QQ&nid=0
If-Modified-Since: Thu, 23 Mar 2023 01:40:24 GMT\r\n
\r\n
[Full request URI: http://www.chinadaily.com.cn/]

[HTTP request 1/6]
[Response in frame: 981]
[Next request in frame: 983]