

Memoria da práctica 2

Wireshark

Pedro Pillado García-Gesto

1.1 - Solicitudes GET básicas

No.	Time	Source	Destination	Protocol	Length	Info
12	2.741462182	192.168.1.51	193.144.61.116	HTTP	478	GET / HTTP/1.1
14	2.886166918	193.144.61.116	192.168.1.51	HTTP	625	HTTP/1.1 301 Moved Permanently
16	2.901810590	192.168.1.51	193.144.61.116	HTTP	481	GET /gl/ HTTP/1.1
22	3.303038377	193.144.61.116	192.168.1.51	HTTP	1018	HTTP/1.1 200 OK (text/html)

1) Que versión do protocolo HTTP solicita o navegador que se use?

Como se ve na imaxe, tanto nas peticións do cliente como nas respostas do servidor figura HTTP 1.1 na versión.

2) Cales son as direccións IP do PC local e do servidor HTTP?

Como se indican nos campos *Source* e *Destination* a ip do PC local é 192.168.1.51 e a do servidor HTTP 193.144.61.116 .

3) Cal é a primeira resposta do servidor HTTP? A que se debe?

A resposta (nº 14) leva o status code 301 Moved Permanently, o que quere decir que se fixo un redireccionamento de URL, indicando que as futuras consultas a esa dirección deberían cambiarse á nova URL á que se redireccionou.

4) ¿Que idiomas lle indica o navegador ao servidor que acepta (se é que indica algún)? Que significa o parámetro 'q=X.Y' nas linguaxes que seguen á primeira opción?

No paquete nº 16 o navegador envía unha nova petición GET na que aparecen listadas as linguas aceptadas polo navegador: galego (gl) e inglés (en-US). Os valores de *q* expresan o peso ponderante de cada unha das opcións, o peso do galego 0.7 e o do inglés 0.3.

```
GET /gl/ HTTP/1.1\r\n
Host: ciencias.udc.es\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: gl,en-US;q=0.7,en;q=0.3\r\n
```

- 5) En que paquete da traza e en que campo se indica o navegador e o sistema operativo que estamos a usar?

```
▶ Frame 12: 478 bytes on wire (3824 bits), 478 bytes captured (3824 bits) on interface wlp3s0,
▶ Ethernet II, Src: IntelCor_b5:70:7f (dc:53:60:b5:70:7f), Dst: AskeyCom_6d:0d:b1 (08:6a:0a:6d
▶ Internet Protocol Version 4, Src: 192.168.1.51, Dst: 193.144.61.116
▶ Transmission Control Protocol, Src Port: 58306, Dst Port: 80, Seq: 1, Ack: 1, Len: 412
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: ciencias.udc.es\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: gl,en-US;q=0.7,en;q=0.3\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
  ▶ Cookie: be40982dcf8e07088f93a1479365cff9=hpd10csubhnhvhn93b8ufk1bi0\r\n
```

Na primeira petición GET (paquete nº12) figuran no campo *User-Agent* a información sobre o sistema operativo (*Linux 64b x86 e Firefox 75.0*).

- 6) Envía o noso navegador algunha cookie? En caso afirmativo, que datos envía?

Explica brevemente algunha desas cookies. En caso de que non aparezan cookies na primeira mensaxe GET, consultar algunha das seguintes peticións.

```
▶ Cookie: be40982dcf8e07088f93a1479365cff9=hpd10csubhnhvhn93b8ufk1bi0\r\n
```

Envíase unha cookie de nome *be40982dcf8e07088f93a1479365cff9* e de valor *hpd10csubhnhvhn93b8ufk1bi0* no paquete 12, a primeira petición GET.

- 7) Canto tempo transcorreu dende que se enviou o primeiro GET ata que se recibiu o OK?

Na imaxe da resposta á pregunta 1 figuran os timestamps do primeiro e último paquete, 2.741462182 e 3.303038377 respectivamente, o que resulta en 0.5615761950000002 segundos.

- 8) Que paquete(s) e campos gardan o código html propiamente da web solicitada?

```
▼ Line-based text data: text/html (238 lines)
<!DOCTYPE HTML>\n
<html lang="gl-es" dir="ltr" data-config='{ "twitter":0, "plusone":0, "facebook":0, "style":"blue'
\n
<head>\n
<meta http-equiv="X-UA-Compatible" content="IE=edge">\n
<meta name="viewport" content="width=device-width, initial-scale=1">\n
<meta charset="utf-8" />\n
<base href="http://ciencias.udc.es/gl/" />\n
<meta name="keywords" content="Facultade, Ciencias, UDC, Sciences, biology biologia, biología;\n
<meta name="description" content="Facultade de Ciencias, UDC" />\n
<title>Benvidos/Benvidas á Facultade de Ciencias</title>\n
<link href="/gl/?format=feed&type=rss" rel="alternate" type="application/rss+xml" title='\n
<link href="/gl/?format=feed&type=atom" rel="alternate" type="application/atom+xml" titl
```

No paquete 22 correspondente á última resposta do servidor figura un campo *Line-based text data*, que, ao ser desplegado revela o dódigo html da páxina.

9) Que software utiliza o servidor HTTP?

Segundo a información que devolve o servidor no paquete 22 no campo *Server* figura o tipo de servidor que se está a empregar, *Apache/2.4.7 (Ubuntu)*.

10) Cando foi modificado por última vez o contido HTML enviado polo servidor? No caso de que se realicen varias peticións de contido ao servidor, indicar só un par de exemplos neste apartado.

```
----- Last-Modified: Wed, 22 Apr 2020 14:56:42 GMT\r\n
```

No paquete 22, no campo *Last-Modified* figura o 22 de abril ás 14:56:42 GMT.

11) Tras o primeiro HTTP OK pódese ver que o navegador analiza o código HTML e realiza novas peticións HTTP GET, ¿Que tipos de datos se intercambian?

Seq	Time	Source	Destination	Process	Length	Info
43	3.192656293	192.168.1.51	193.144.61.116	HTTP	409	GET / HTTP/1.1
47	3.359418061	193.144.61.116	192.168.1.51	HTTP	716	HTTP/1.1 301 Moved Permanently
49	3.394336313	192.168.1.51	193.144.61.116	HTTP	481	GET /gl/ HTTP/1.1
64	3.467605074	192.168.1.51	93.184.220.29	OCSP	454	[TCP Previous segment not captured] Request
65	3.481537812	93.184.220.29	192.168.1.51	OCSP	864	[TCP ACKed unseen segment] Response
91	3.845836432	193.144.61.116	192.168.1.51	HTTP	1018	HTTP/1.1 200 OK (text/html)
118	4.064458889	192.168.1.51	193.144.61.116	HTTP	496	GET /plugins/system/jce/css/content.css?9d038f703775c720
126	4.104804114	192.168.1.51	193.144.61.116	HTTP	473	GET /media/jui/js/jquery.min.js?9d038f703775c720
129	4.105835924	192.168.1.51	193.144.61.116	HTTP	481	GET /media/jui/js/jquery-migrate.min.js?9d038f703775c720
132	4.106619807	192.168.1.51	193.144.61.116	HTTP	448	GET /media/widgetkit/uikit2-304edd0d.js HTTP/1.1
135	4.107471348	192.168.1.51	193.144.61.116	HTTP	452	GET /media/widgetkit/wk-scripts-e80b7146.js HTTP/1.1
139	4.108169262	192.168.1.51	193.144.61.116	HTTP	480	GET /media/jui/js/jquery.noconflict.js?9d038f703775c720
140	4.108785550	193.144.61.116	192.168.1.51	HTTP	764	HTTP/1.1 200 OK (text/css)
142	4.109178280	192.168.1.51	193.144.61.116	HTTP	475	GET /templates/yoo_avenue/styles/blue/css/theme.css
154	4.154101260	193.144.61.116	192.168.1.51	HTTP	111	HTTP/1.1 200 OK (application/javascript)
156	4.154418864	192.168.1.51	193.144.61.116	HTTP	464	GET /templates/yoo_avenue/css/custom.css HTTP/1.1
159	4.155493458	193.144.61.116	192.168.1.51	HTTP	382	HTTP/1.1 200 OK (application/javascript)
161	4.155941845	192.168.1.51	193.144.61.116	HTTP	464	GET /templates/yoo_avenue/war/vendor/uikit/js/uikit.js

Pódese ver que tras enviar o primeiro GET envíanse outros gets para solicitar diferente contido multimedia da páxina.

1.2 - Solicitudes GET condicionais

- 1) **Inspecciona o contido das mensaxes GET onde se solicitan os obxectos da web á primeira vez que se carga a páxina, Aparece algunha liña coa cabeceira “If-Modified-Since:”?**

Tras baleirar a cache ningunha das solicitudes get que envía o navegador inclúe a cabeceira *If-Modified-Since* xa que o navegador non ten información previa da páxina, e polo tanto vai ter que cargar todos os elementos da páxina, xa que non ten cacheados ningún dos elementos.

- 2) **Vendo os HTTP GET relacionados coa recarga da web, aparece agora unha liña “If-Modified-Since:”? En caso afirmativo, que información acompaña a dita cabeceira “If-Modified-Since:”?**

A partir da segunda carga da páxina, o navegador xa gardou datos dela na cache, polo tanto todas as peticións inclúen unha cabeceira *If-Modified-Since* cuxo contido é a data do último acceso á web, para que, de ser o contido anterior á data se obterían os novos contidos.

- 3) **Que status code e response phrase devolve o servidor HTTP en resposta aos GET relacionados cos obxectos embebidos no HTML?**

```
HTTP/1.1 304 Not Modified\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 304 Not Modified\r\n]
    Response Version: HTTP/1.1
    Status Code: 304
    [Status Code Description: Not Modified]
```

Responden co código 304:Not Modified, que indican que a última data de modificación dos contidos son anteriores á data de If-Modified-Since, e polo tanto a copia da cache coincide coa actual e non fai falta obter os contidos outra vez.

1.3 - Autenticación Básica

- 1) **Que status code devolve o servidor ao primeiro HTTP GET?**

```
Hypertext Transfer Protocol
  HTTP/1.1 401 Unauthorized\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 401 Unauthorized\r\n]
      Response Version: HTTP/1.1
      Status Code: 401
      [Status Code Description: Unauthorized]
      Response Phrase: Unauthorized
      Date: Fri, 24 Apr 2020 14:58:04 GMT\r\n
      Server: Apache\r\n
```

O servidor responde cun 401: Unauthorized, indicando que para obter o contido solicitado é preciso autenticarse.

- 2) Á vista dos seguintes HTTP GET que se envían ao servidor, que campo novo se inclúe na mensaxe correspondente á petición de autenticación? Buscar unha resposta do servidor co código 200 OK e mirar o GET correspondente.

```
▼ Hypertext Transfer Protocol
  ▼ GET /keeper/mystash/secretstuff.html HTTP/1.1\r\n
    ▶ [Expert Info (Chat/Sequence): GET /keeper/mystash/secretstuff.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /keeper/mystash/secretstuff.html
      Request Version: HTTP/1.1
      Host: www.pagetutor.com\r\n
      User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
      Accept-Language: gl,en-US;q=0.7,en;q=0.3\r\n
      Accept-Encoding: gzip, deflate\r\n
      DNT: 1\r\n
      Connection: keep-alive\r\n
      Upgrade-Insecure-Requests: 1\r\n
  ▼ Authorization: Basic amltbXk6cGFnZQ==\r\n
    Credentials: jimmy:page
  \r\n
```

Inclúese un novo campo chamado “*Authorization*”, co contido das credenciais requiridas.