

Aprendiendo un poco más de HTTP

El presente documento es complementario a lo visto en las clases teóricas y el laboratorio de protocolos de capa de aplicación. El curso de Redes de Datos 1 es autocontenido entre el teórico y los laboratorios, el material complementario busca ofrecer herramientas para que los alumnos puedan profundizar o complementar sus conocimientos por cuenta propia.

Introducción: Sin necesidad de utilizar el Wireshark es posible obtener información del intercambio de la descarga de una página web, las peticiones intercambiadas y la respuesta.

A continuación, se explica cómo utilizar el propio navegador para poder realizarlo, cuenta con la ventaja que si bien el intercambio puede realizarse por https (se encuentra encriptado), es posible realizar un análisis sin conocer la clave privada del certificado.

Para cada uno de los navegadores se explica el procedimiento para ingresar al modo desarrollador en el cual se puede visualizar, entre otras cosas, el intercambio de peticiones HTTP y sus respuestas.

Firefox: Ctrl+Shift+E

The screenshot shows the Firefox browser with the Developer Tools network tab open. The page is 'BANCO REPUBLICA' and the URL is 'https://www.brou.com.uy'. The network tab displays a list of requests, with the selected request being a GET request for 'jquery.cycle2.js'. The response headers for this request are visible on the right side of the network panel.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.brou.com.uy	funciones.js		script	cached	0 B
200	GET	www.brou.com.uy	main.css?browserid=firefox&themeld=brouareas_WAR_brouar...		stylesheet	Blocked	
200	GET	www.brou.com.uy	jquery.cycle2.js		script	cached	0 B
200	GET	www.brou.com.uy	imagesloaded.pkgd.js		script	cached	0 B
200	GET	www.brou.com.uy	bootstrap.min.js		script	cached	0 B
200	GET	www.brou.com.uy	company_logo?img_id=77868&t=1593607442575		img	Blocked	
200	GET	www.brou.com.uy	iconmobile.png		img	Blocked	
200	GET	www.brou.com.uy	layout_icon?img_id=106381&t=1593607443152		img	Blocked	
200	GET	www.brou.com.uy	layout_icon?img_id=106386&t=1593607443152		img	Blocked	
200	GET	www.brou.com.uy	7c97f31e-5679-4689-ae1f-4d510f6aac2b7f+1567148337513		img	Blocked	
200	GET	www.brou.com.uy	2431edb1-2d07-4110-a09d-4a73bb9f3b84?i=15918071405...		img	Blocked	
200	GET	www.brou.com.uy	a6a2e1f4-9a88-4e0d-b490-1e7c71f6e64d?i=1593541822792		img	Blocked	
200	GET	www.brou.com.uy	ac2e709b-6494-4d06-bfb0-4410637c235c?i=15844775395...		img	Blocked	
200	GET	www.brou.com.uy	fe27f865-bf0c-4546-97e9-48f5c5c8804?i=15843005997189		img	Blocked	
200	GET	www.brou.com.uy	logo-ebrou.png		img	Blocked	
200	GET	www.brou.com.uy	bc74557f-5183-47ed-a5b9-25c3444e9d9?i=1532558105020		img	Blocked	
200	GET	www.brou.com.uy	fbab773e9-af1a6-d7f6f-83f6-bb854686d43ac?i=15952674962		img	Blocked	

The selected request details show the following response headers:

- Status: 200 OK
- Version: HTTP/1.1
- Transferred: 65.49 KB (0 B size)
- Referrer Policy: no-referrer-when-downgrade
- Response Headers (649 B):
 - Accept-Ranges: bytes
 - Cache-Control: max-age=31536000, public
 - Connection: Keep-Alive
 - Content-Encoding: gzip
 - Content-Length: 9033
 - Content-Type: text/javascript
 - Date: Wed, 19 Aug 2020 23:19:07 GMT
 - ETag: W/45217-1518102868000
 - Expires: Sat, 17 Aug 2030 23:19:07 GMT
 - filter-class: com.liferay.portal.servlet.filters.header.HeaderFilter
 - Keep-Alive: timeout=120, max=798
 - Last-Modified: Thu, 08 Feb 2018 15:14:28 GMT
 - Server: Apache

Chrome: Ctrl+Shift+I

The screenshot shows the Chrome DevTools Network tab. The selected request is a GET request to `https://www.brou.com.uy/personas/inicio`. The status is 200 OK. The response headers include `Cache-Control: private, no-cache, no-store, must-revalidate`, `Connection: Keep-Alive`, `Content-Encoding: gzip`, `Content-Type: text/html; charset=UTF-8`, `Date: Wed, 26 Aug 2020 22:41:01 GMT`, `Expires: Thu, 01 Jan 1970 00:00:00 GMT`, `Keep-Alive: timeout=120, max=790`, and `Pragma: no-cache`. The response body is not visible, but the headers are expanded.

Internet Explorer: Fn+F12

The screenshot shows the Internet Explorer Developer Tools Network tab. The selected request is a GET request to `https://www.brou.com.uy/`. The status is 200 OK. The response headers include `Cache-Control: private, no-cache, no-store, must-revalidate`, `Connection: Keep-Alive`, `Content-Encoding: gzip`, `Content-Type: text/html; charset=UTF-8`, `Date: Wed, 26 Aug 2020 22:41:01 GMT`, `Expires: Thu, 01 Jan 1970 00:00:00 GMT`, `Keep-Alive: timeout=120, max=790`, and `Pragma: no-cache`. The response body is not visible, but the headers are expanded.

Nombre / Ruta de acceso	Protocolo	Método	Resultado / Descripción	Tipo de contenido	Recibido	Tiempo	Iniciador / Tipo
vevent7an_audIt=0&referrer=http%3A%2F%2Fwww... https://nym1-ib.adms.com/	HTTPS	GET	200 OK	text/html	0 B	1,17 s	XMLHttpRequest
https://nym1-ib.adms.com/	HTTPS	CONN...	200 Connection estab...			455,61 ms	
vevent7an_audIt=0&referrer=http%3A%2F%2Fwww... https://nym1-ib.adms.com/	HTTPS	GET	200 OK	text/html	0 B	241,57 ms	XMLHttpRequest
vevent7an_audIt=0&e=wqT_3QKGA3yGAQAAAwD... https://nym1-ib.adms.com/	HTTPS	GET	200 OK	text/html	0 B	235,71 ms	XMLHttpRequest
vevent7an_audIt=0&e=wqT_3QKGA3yGAQAAAwD... https://nym1-ib.adms.com/	HTTPS	GET	200 OK	text/html	0 B	250,82 ms	XMLHttpRequest
http://www.brou.com.uy/	HTTP	GET	301 Moved Perman...	text/html	232 B	168,98 ms	document
https://www.brou.com.uy/	HTTPS	GET	200 OK	text/html		444,09 ms	document
https://www.brou.com.uy/	HTTPS	CONN...	200 Connection estab...			100,55 ms	
aii.css?browserId=ie&themeId=brouareas_WAR_br... https://www.brou.com.uy/	HTTPS	GET	200	text/css	26,29 KB	187,34 ms	www.brou.com.uy:1

Microsoft Edge: Fn+F12

The screenshot shows the Microsoft Edge browser interface. The address bar displays the URL <https://www.brou.com.uy/>. The page content includes the Banco República logo, a navigation menu, and a main banner for 'Agendá la atención presencial de tu empresa'. Below the banner, there are sections for 'Adhesión a eBROU', 'Acceso a eBROU', 'Cotizaciones', and 'Noticias del BROU'. The developer tools are open, showing the 'Red' (Network) tab. The network log displays a list of requests, including CSS files and XSPX files. The selected request is a GET request to <https://www.bing.com/rb/5/cir2.cc.nc/>. The response headers are visible, including 'Cache-Control: public, max-age=432000', 'Content-Type: text/css; charset=utf-8', and 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) ...'.

Desafío: Investigue el intercambio de peticiones HTTP y las respuestas.

Averigüe la utilidad de los siguientes headers opcionales que acompañan a una petición GET:

- Connection:
- Cookie:
- User-Agent: