

# ANÁLISIS DE RED CON WIRESHARK Y NMAP

---

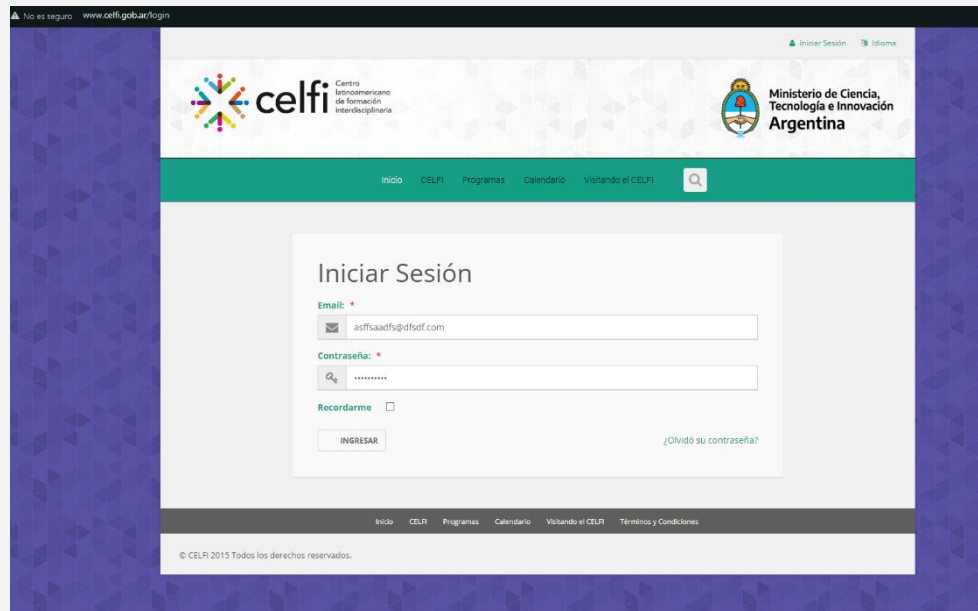


---

SEGURIDAD INFORMÁTICA  
JUAN CARLOS NAVIDAD GARCÍA

## 1. Creación del paquete:

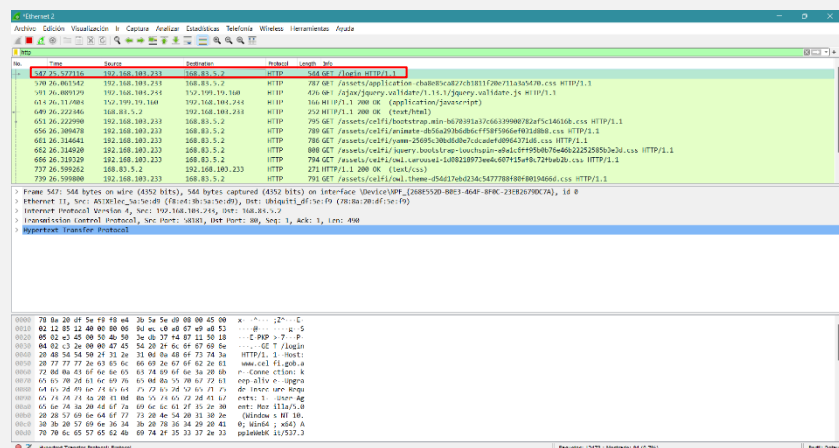
Lo primero que haremos será navegar por internet y realizar una solicitud de inicio de sesión sobre una página sin protección HTTP, de esta manera podremos ver toda la información del paquete que se crea en la red al intentar iniciar sesión en una página:



## 2. Comprobación con Wireshark:

Ahora lo que haremos será abrir Wireshark para poder comprobar si se ha registrado el paquete. Para poder capturar el tráfico en la red, deberemos de iniciar Wireshark como administrador y seleccionar la tarjeta de red con la que estamos conectados.

Como el paquete que queremos ver es sobre una página HTTP, aplicaremos el primer filtro de búsqueda como HTTP:



Si queremos saber más acerca del paquete y de la web donde se ha iniciado sesión, haremos click derecho sobre el paquete → Seguir → Flujo HTTP:

Marcar/Desmarcar paquete	Control+M	/celfi/animate-db56a293b6db6c7f58f5966ef031d8
Ignorar/No ignorar paquete	Control+D	/celfi/yamm-25695c38bd6d0e7cdcadef0964371d6.4
Establecer/Anular referencia de tiempo	Control+T	/celfi/jquery.bootstrap-touchspin-a9a1c6ff95b1
Modificar horario...	Control+Mayúsculas+T	/celfi/owl.carousel-1d08218973ee4c607f15af8c7:
Comentario de paquete...	Control+Alt+C	) OK (text/css)
Editar nombre resuelto		) OK (text/css)
Aplicar como filtro		/celfi/owl.theme-d54d17ebd234c5477788f80f8019:
Prepare as Filter		/celfi/owl.transitions-5bcb4b16d69b0eae2b4fa
Filtro de conversación		) OK (text/css)
Colorear conversación		/celfi/owl.carousel-1d08218973ee4c607f15af8c7:
SCTP		) OK (text/css)
Seguir		th0, id 0
Copiar		0:12:35:02)
Protocol Preferences		
Decode As...		
Mostrar paquete en nueva ventana		
	Flujo TCP	Control+Alt+Mayúsculas+T
	Flujo UDP	Control+Alt+Mayúsculas+U
	Flujo TLS	Control+Alt+Mayúsculas+S
	Flujo HTTP	Control+Alt+Mayúsculas+H
	Flujo HTTP/2	
	Flujo QUIC	

```

Wireshark - Seguir flujo HTTP (tcpstream eq 6) - Ethernet 2

GET /login HTTP/1.1
Host: www.celfi.gov.ar
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36 OPR/83.0.4254.46
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=0.9
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Status: 200 OK
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: POST, PUT, DELETE, GET, OPTIONS
Access-Control-Request-Method: *
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accept, Authorization
ETag: "498a6c13d3adab7e5244c72e6e2da2a1"
Cache-Control: max-age=0, private, must-revalidate
Set-Cookie: _celfics_session=N1hMa0VzeEMxYnhSalUzjdVR6RFQvRzVxOFVFK3ZUTGVPREpFMtyRFZ1Vhphb2t2T2pJ51A0aTdUUDZraXdl2ZUxVQ3N3ckNTUkpYK0J1Vjdub2FY1pU0FVycHhhaXhXcmprwajMTzRLlmlhrQm1VQkVZaVlac3A2dEdmZjc2UUtPMDJjMERqeT8nV1NpOXVcVVRQOQoyUm1tdHRFY2h2MetteFc0bTFmM3FjPS0tMnhvZS9zaTNua281ZjZj3L3FkdhPQ0T09--1706c7f709ee48a420af4b8c3eab9512fc266906; path=/; HttpOnly
X-Request-Id: a2134ad7-3869-42c2-926d-329c74dac38c
X-RunTime: 0.139236
X-Powered-By: Phusion Passenger 4.0.58
Date: Fri, 18 Feb 2022 12:59:55 GMT
Server: nginx/1.6.2 + Phusion Passenger 4.0.58
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET, POST, OPTIONS
Access-Control-Allow-Headers: DNT,X-ReqToken,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,X-FooApp-Auth-Token

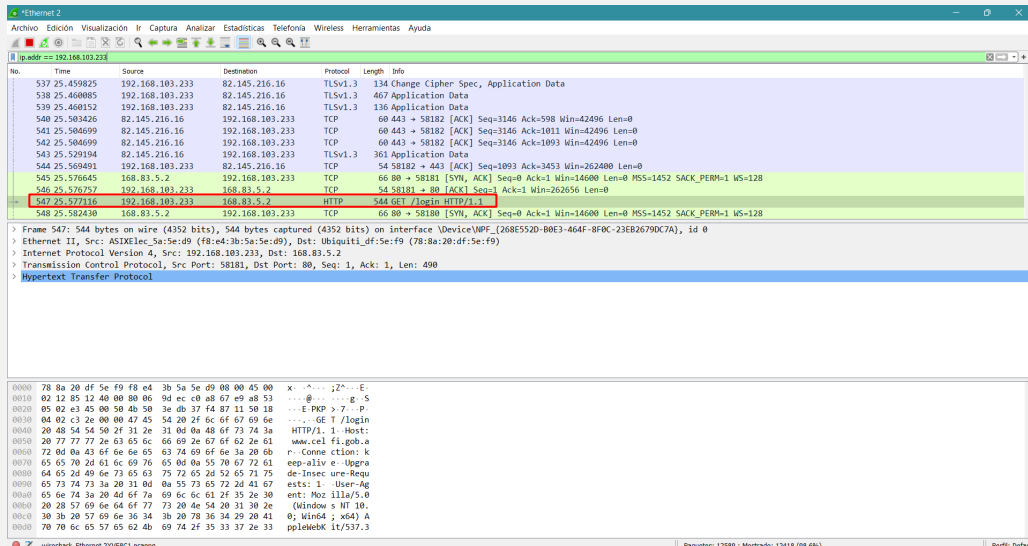
<!DOCTYPE html>
<html>

Paquete 649.12 cliente pkt.11 servidor pkt.21 cambios: Clic para seleccionar.
Conversación completa (1071 kb)
Mostrar datos como ASCII
Buscar:
Filtrar esta secuencia Imprimir Guardar como... Atrás Cerrar Ayuda
  
```

También podemos buscar por dirección IP, le aplicaremos el filtro de búsqueda:

- ip.addr == <IP>

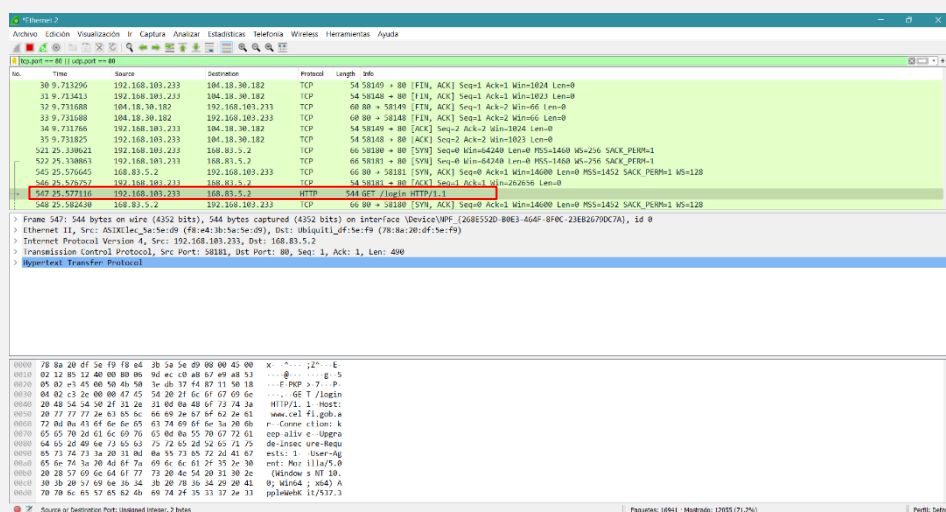
He buscado la misma IP con la que he realizado el inicio de sesión con la página HTTP, nos damos cuenta de que también aparece el paquete anterior:



Entre otros filtros de búsqueda, también podemos filtrar por puertos con:

- tcp/udp.port == <puerto>

En mi caso he filtrado el puerto 80 que es el puerto HTTP para volver a encontrar el paquete de inicio de sesión anterior:



### 3. Comprobación con Nmap:

Lo que vamos a hacer con Nmap es ver si una página está activa y los puertos que tiene abiertos y funcionando, para eso hay dos comandos:

- `nmap -sV <dominio/ip>`
- `nmap -Pn <dominio/ip>`

Primero lo comprobaré con la misma página de Los Cerros y después con la que hemos iniciado sesión anteriormente con el protocolo HTTP:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~[~]  
$ nmap -sV loscerros.org  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-18 08:01 EST  
Nmap scan report for loscerros.org (86.109.166.214)  
Host is up (0.025s latency).  
rDNS record for 86.109.166.214: a0209.abansys.com  
Not shown: 987 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          ProFTPD  
25/tcp    open  smtp         Postfix smtpd  
80/tcp    open  http         nginx  
106/tcp   open  tcpwrapped  
110/tcp   open  pop3         Dovecot pop3d  
143/tcp   open  imap         Dovecot imapd  
443/tcp   open  ssl/http     nginx  
465/tcp   open  ssl/smtp     Postfix smtpd  
587/tcp   open  smtp         Postfix smtpd  
993/tcp   open  ssl/imap     Dovecot imapd  
995/tcp   open  ssl/pop3     Dovecot pop3d  
3306/tcp  open  mysql        MySQL 5.5.5-10.2.33-MariaDB  
8443/tcp  open  ssl/https-alt sw-cp-server  
1 service unrecognized despite returning data. If you know the service/version,  
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit  
.cgi?new-service :  
SF-Port8443-TCP:V=7.92%T=SSL%I=7%D=2/18%Time=620F98C7%P=x86_64-pc-linux-gn  
SF:u%r(GetRequest,20E,"HTTP/1.1"x20303"x20See"x20Other\r\nServer:\x20sw-c
```

```
(kali@kali-vb)~[~]  
$ nmap -Pn celfi.gob.ar  
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-02-18 16:34 CET  
Nmap scan report for celfi.gob.ar (200.9.244.165)  
Host is up (0.27s latency).  
Not shown: 995 filtered ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
110/tcp   open  pop3  
8291/tcp  open  unknown  
  
Nmap done: 1 IP address (1 host up) scanned in 15.37 seconds  
  
(kali@kali-vb)~[~]  
$
```