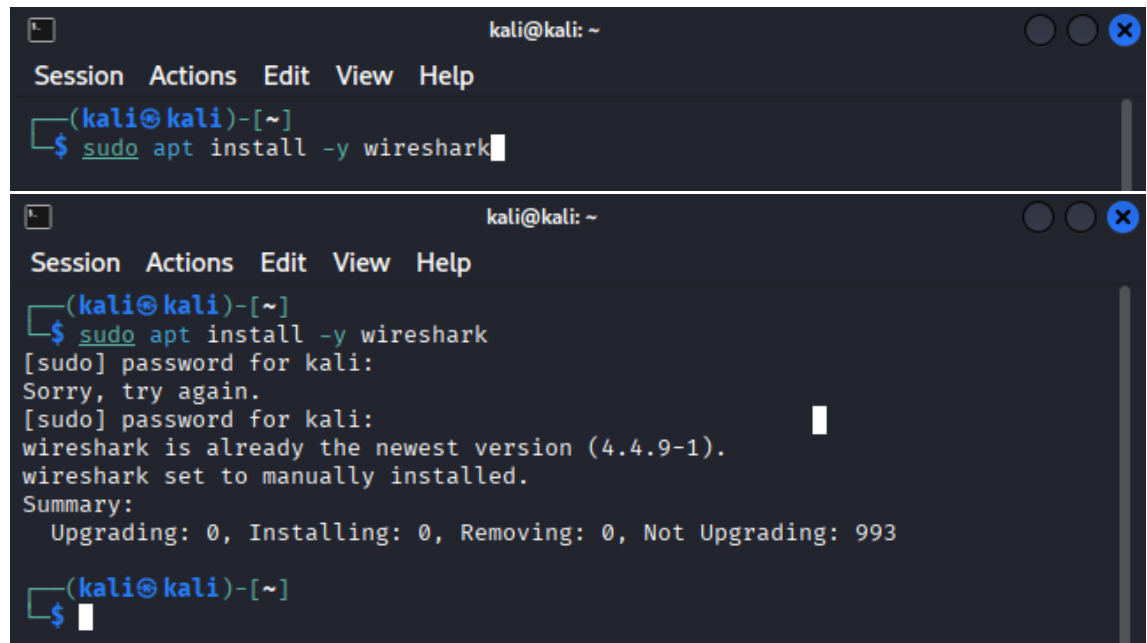


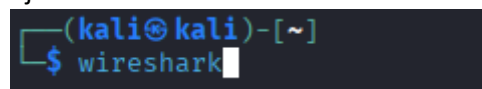
Mario Mendoza

Instalamos wireshark



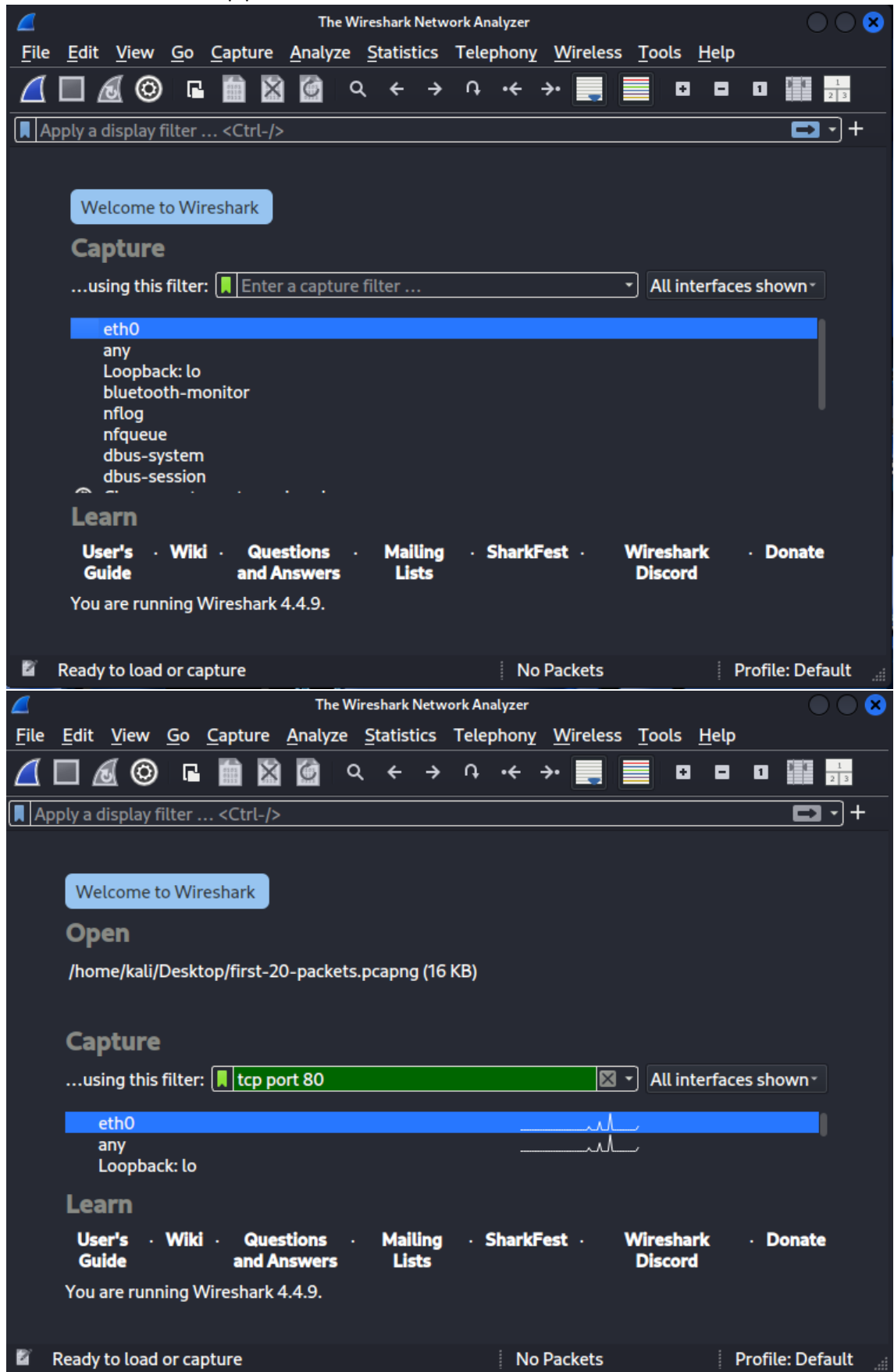
```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt install -y wireshark  
  
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt install -y wireshark  
[sudo] password for kali:  
Sorry, try again.  
[sudo] password for kali:  
wireshark is already the newest version (4.4.9-1).  
wireshark set to manually installed.  
Summary:  
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 993  
  
(kali@kali)-[~]  
$
```

Ejecutamos wireshark

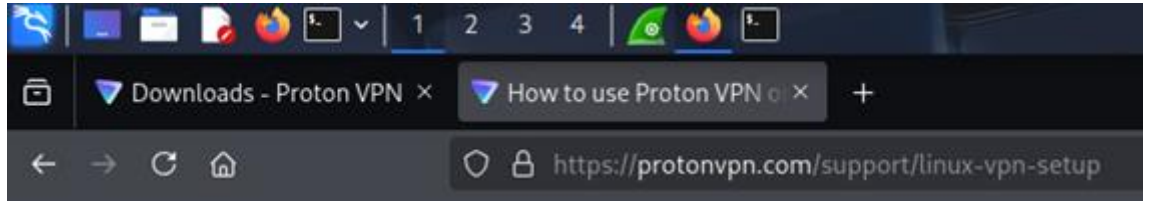


```
(kali@kali)-[~]  
$ wireshark
```

En el filtro añadimos: tcp port 80



Abrimos una pagina en internet y esperamos a que se envíen los paquetes



Iniciamos y esperamos a capturar 20 paquetes

Capturing from eth0 (tcp port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	192.124.249.22	TCP	74	347
2	0.000319178	10.0.2.15	192.124.249.22	TCP	74	347
3	0.027634996	192.124.249.22	10.0.2.15	TCP	60	80
4	0.027662753	10.0.2.15	192.124.249.22	TCP	54	347
5	0.028127769	10.0.2.15	192.124.249.22	OCSP	482	Req
6	0.028300798	192.124.249.22	10.0.2.15	TCP	60	80
7	0.250406008	10.0.2.15	192.124.249.22	TCP	74	347
8	0.277930941	192.124.249.22	10.0.2.15	TCP	60	80
9	0.277958282	10.0.2.15	192.124.249.22	TCP	54	347
10	0.278526859	10.0.2.15	192.124.249.22	OCSP	482	Req
11	0.278700820	192.124.249.22	10.0.2.15	TCP	60	80

Frame 1: 74 bytes on wire (592 bits), 70 captured (560 bits) on interface eth0
Ethernet II, Src: PCSSystemtec_1f:b7:23, Dst: 08:00:27:1c:3e:00
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 192.124.249.22
Transmission Control Protocol, Src Port: 347, Dst Port: 80

eth0: <live capture in progress> Packets: 52 Profile: Default

*eth0 (tcp port 80)

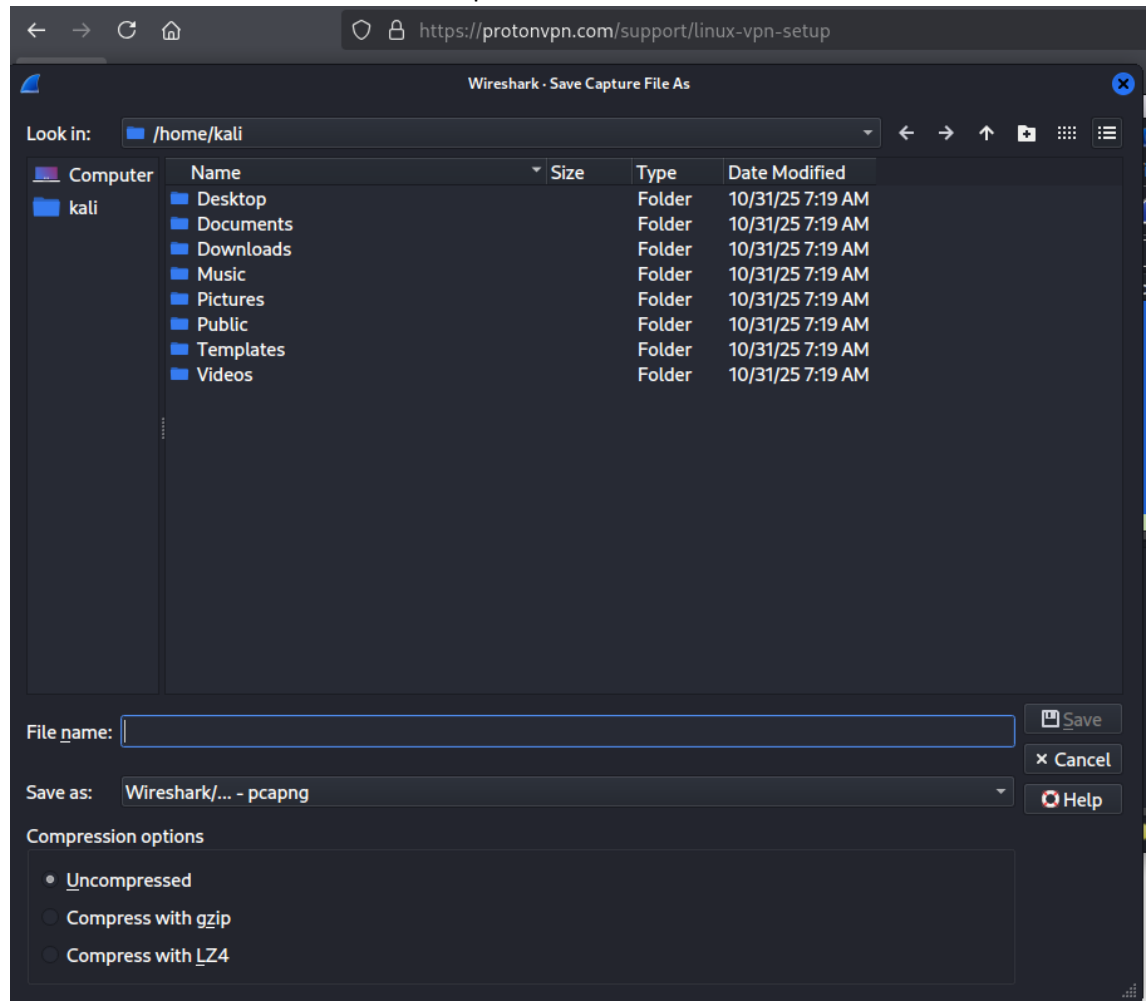
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
11	0.278700820	192.124.249.22	10.0.2.15	TCP	60	80
12	0.324736666	192.124.249.22	10.0.2.15	TCP	1494	
13	0.324737297	192.124.249.22	10.0.2.15	OCSP	1333	
14	0.324761655	10.0.2.15	192.124.249.22	TCP	54	
15	0.324807723	10.0.2.15	192.124.249.22	TCP	54	
16	0.335157401	192.124.249.22	10.0.2.15	TCP	1494	
17	0.335157727	192.124.249.22	10.0.2.15	OCSP	1333	
18	0.335179018	10.0.2.15	192.124.249.22	TCP	54	
19	0.335222641	10.0.2.15	192.124.249.22	TCP	54	
20	1.023260207	192.124.249.22	10.0.2.15	TCP	60	
21	1.023325967	10.0.2.15	192.124.249.22	TCP	54	

wireshark_...6F3.pcapng Packets: 92 · Selected: 20 (21.7%) · Dropped: 0 (0.0%) Profile: Default

Guardamos el documento en el desktop



Listo para analizar luego



Usamos el siguiente comando para analizar los puertos del servidor (Kali)

```
(kali@kali)-[~]  
$ nmap -sV scanne.nmap.com
```

Resultado del análisis:

```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV scanne.nmap.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-14 07:09 EST  
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan  
SYN Stealth Scan Timing: About 51.93% done; ETC: 07:09 (0:00:11 remaining)  
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 99.44% done; ETC: 07:09 (0:00:00 remaining)  
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan  
NSE Timing: About 87.50% done; ETC: 07:09 (0:00:00 remaining)  
Nmap scan report for scanne.nmap.com (50.116.1.184)  
Host is up (0.020s latency).  
rDNS record for 50.116.1.184: ack.nmap.org  
Not shown: 995 filtered tcp ports (no-response)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)  
25/tcp    open  smtp     Postfix smtpd  
80/tcp    open  http     Apache httpd 2.4.6  
113/tcp   closed ident  
443/tcp   open  ssl/https Apache/2.4.6 (CentOS)  
Service Info: Host: ack.nmap.org  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 44.93 seconds  
  
(kali@kali)-[~]  
$
```