UNIVERSIDAD DEL VALLE DE GUATEMALA

Facultad de Ingeniería

Redes – Jorge Yaz

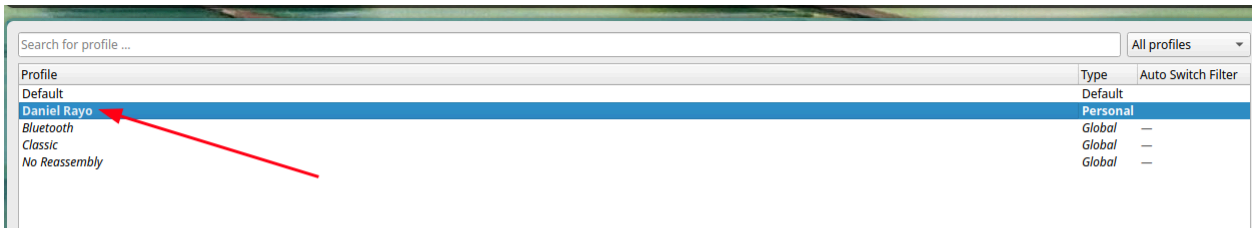
Lab 1

Daniel Alfredo Rayo Roldán, 22933

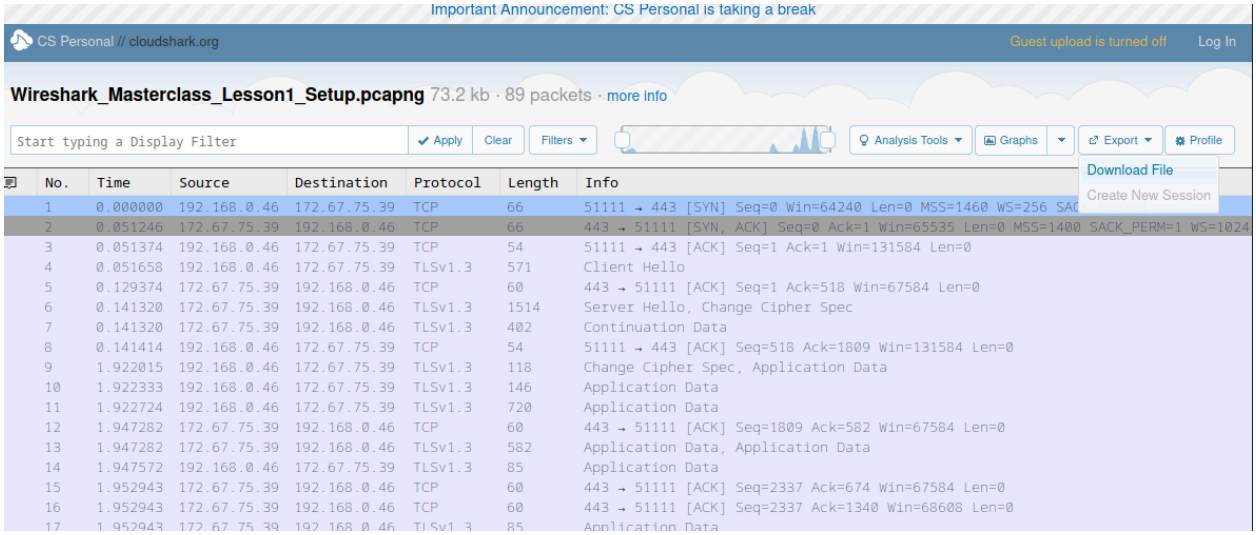
Wireshark

1.1 Personalización del entorno

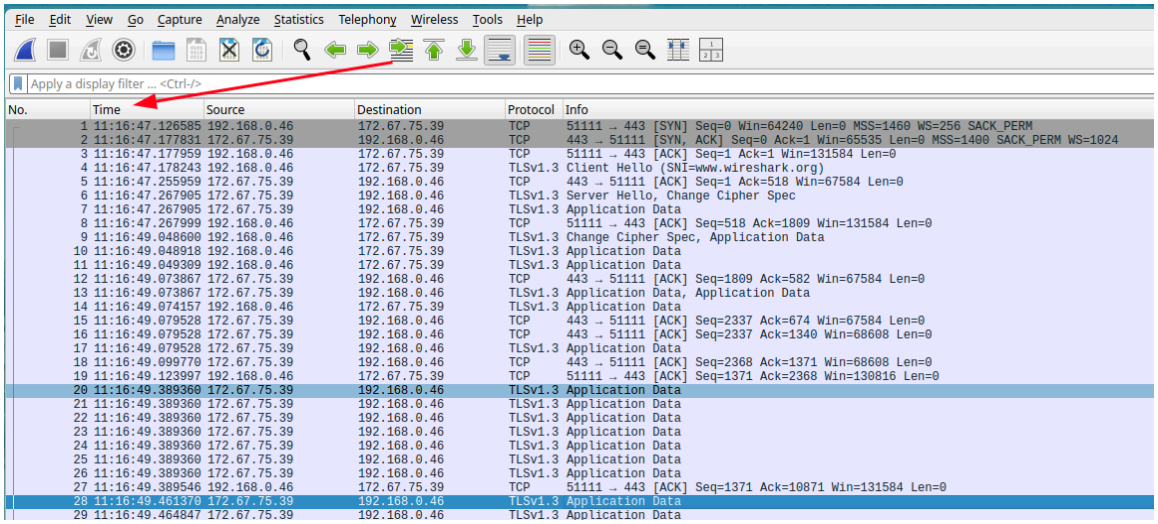
Cree un perfil con su primer nombre y primer apellido (edit -> configuration profile)



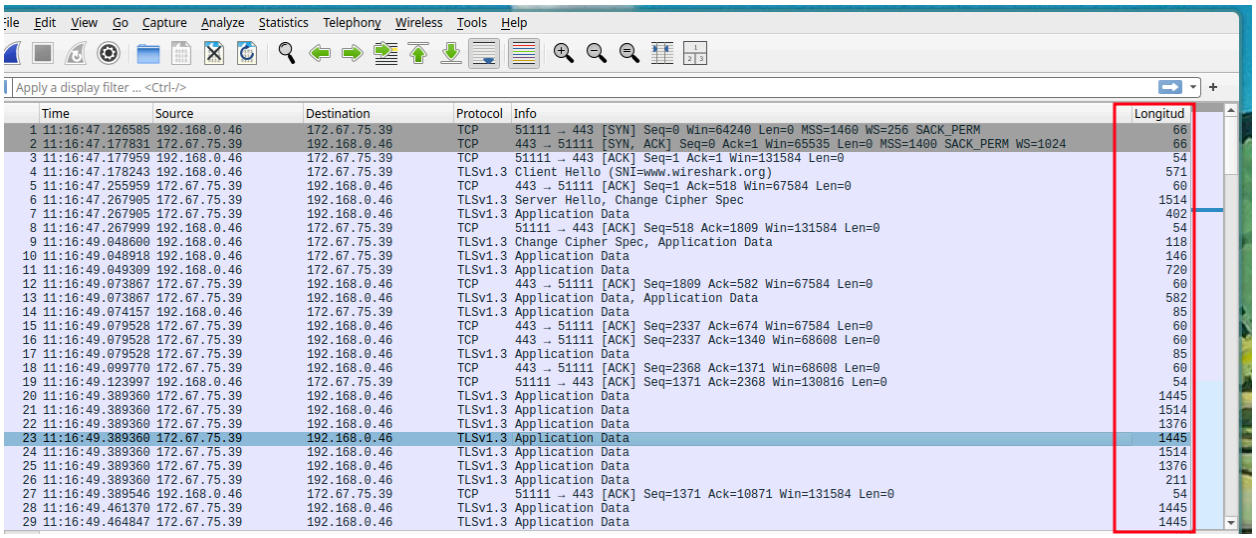
Descargue el archivo https://www.cloudshark.org/captures/e6fb36096dbb (Export -> Download)



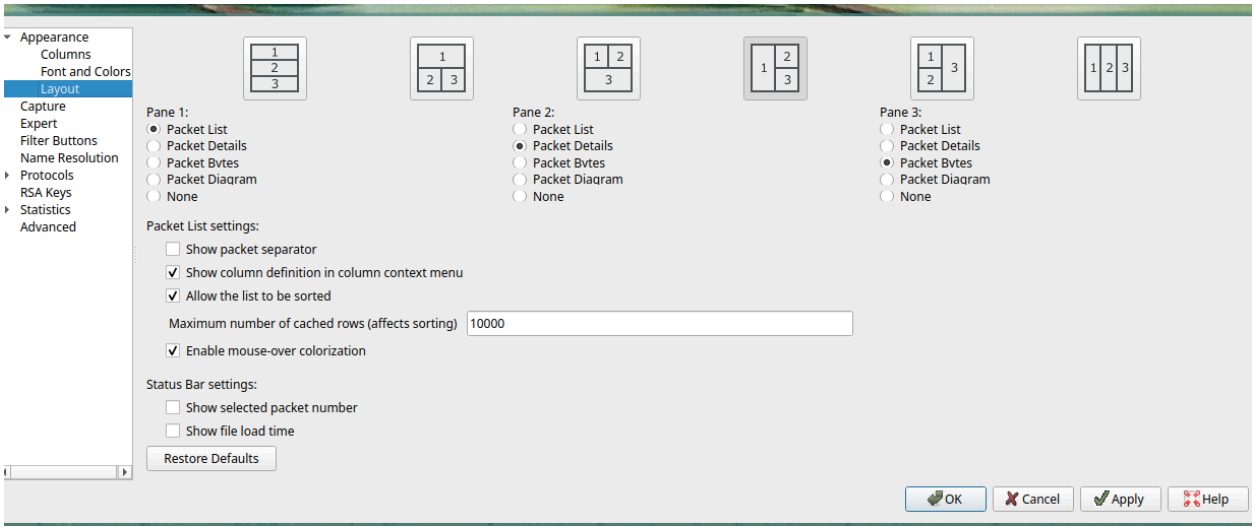
Aplique el formato de tiempo Time of Day (view -> Time Display Format)



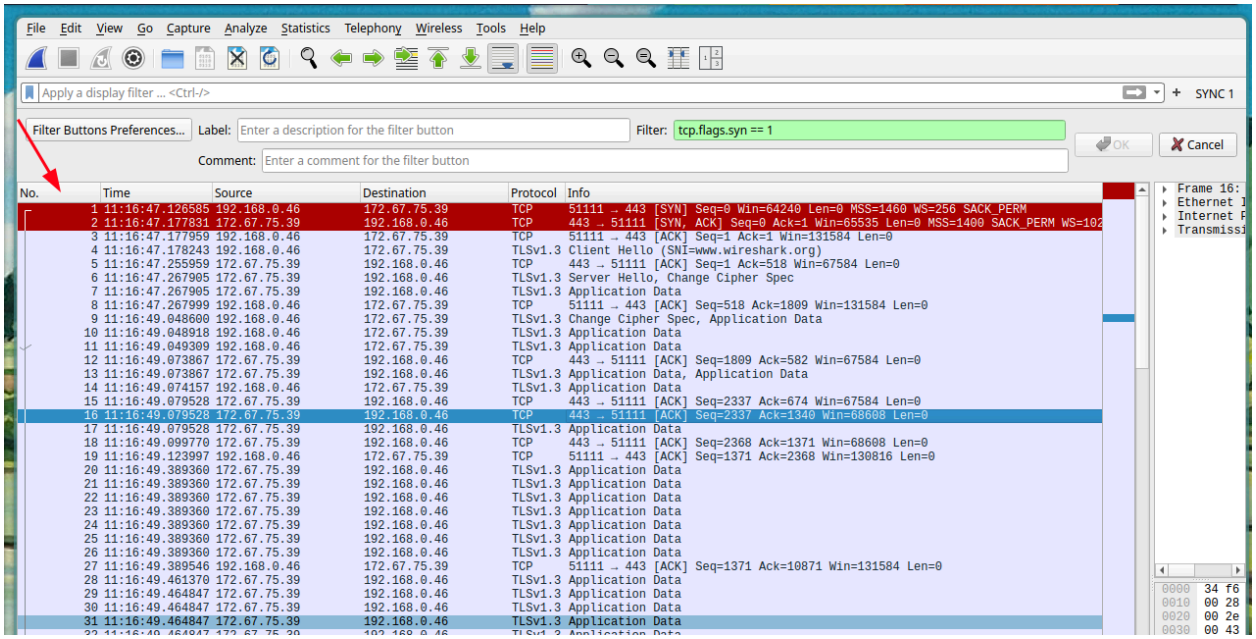
Agregue una columna con la longitud del protocolo (preferences -> column -> +)



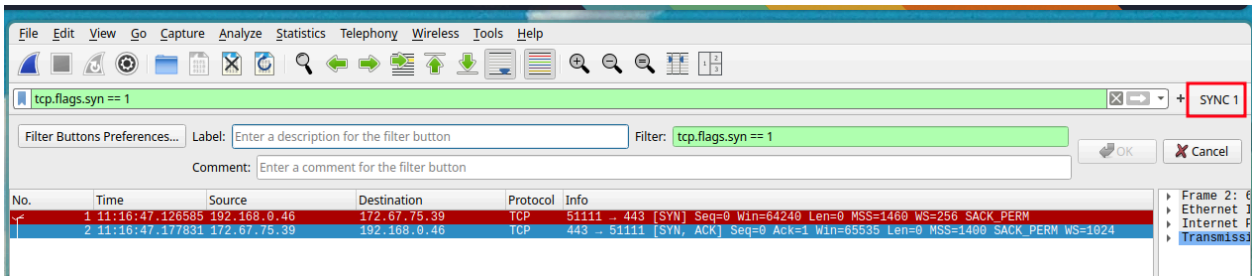
Aplique un esquema de paneles que sea de su preferencia (que no sea el esquema por defecto) (preferences -> Layout)


Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Pane 1:
Packet List
Packet Details
Packet Bytes
Packet Diagram
None
Pane 2:
Packet List
Packet Details
Packet Bytes
Packet Diagram
None
Pane 3:
Packet List
Packet Details
Packet Bytes
Packet Diagram
None
Packet List settings:
Show packet separator
Show column definition in column context menu
Allow the list to be sorted
Maximum number of cached rows (affects sorting)
10000
Enable mouse-over colorization
Status Bar settings:
Show selected packet number
Show file load time
Restore Defaults
OK
Cancel
Apply
Help

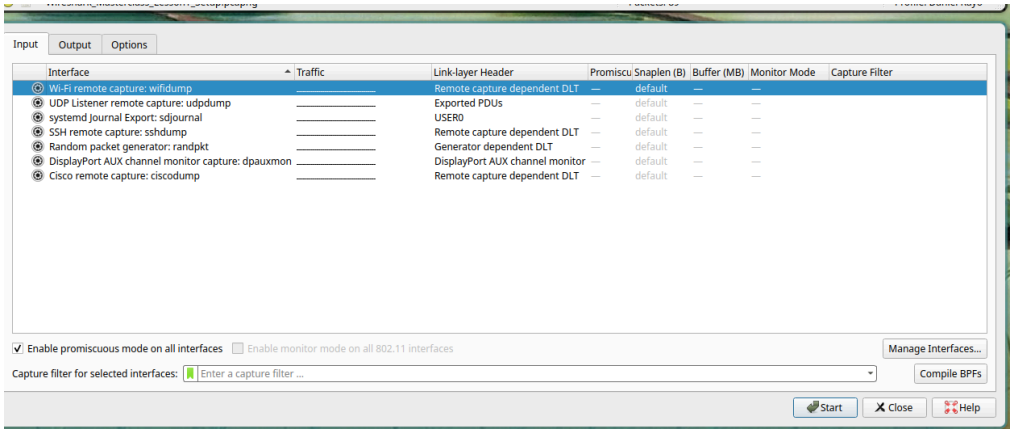
Aplique una regla de color para el protocolo TCP cuyas banderas SYN sean iguales a 1, y coloque el color de su preferencia. (View -> coloring rules -> +)



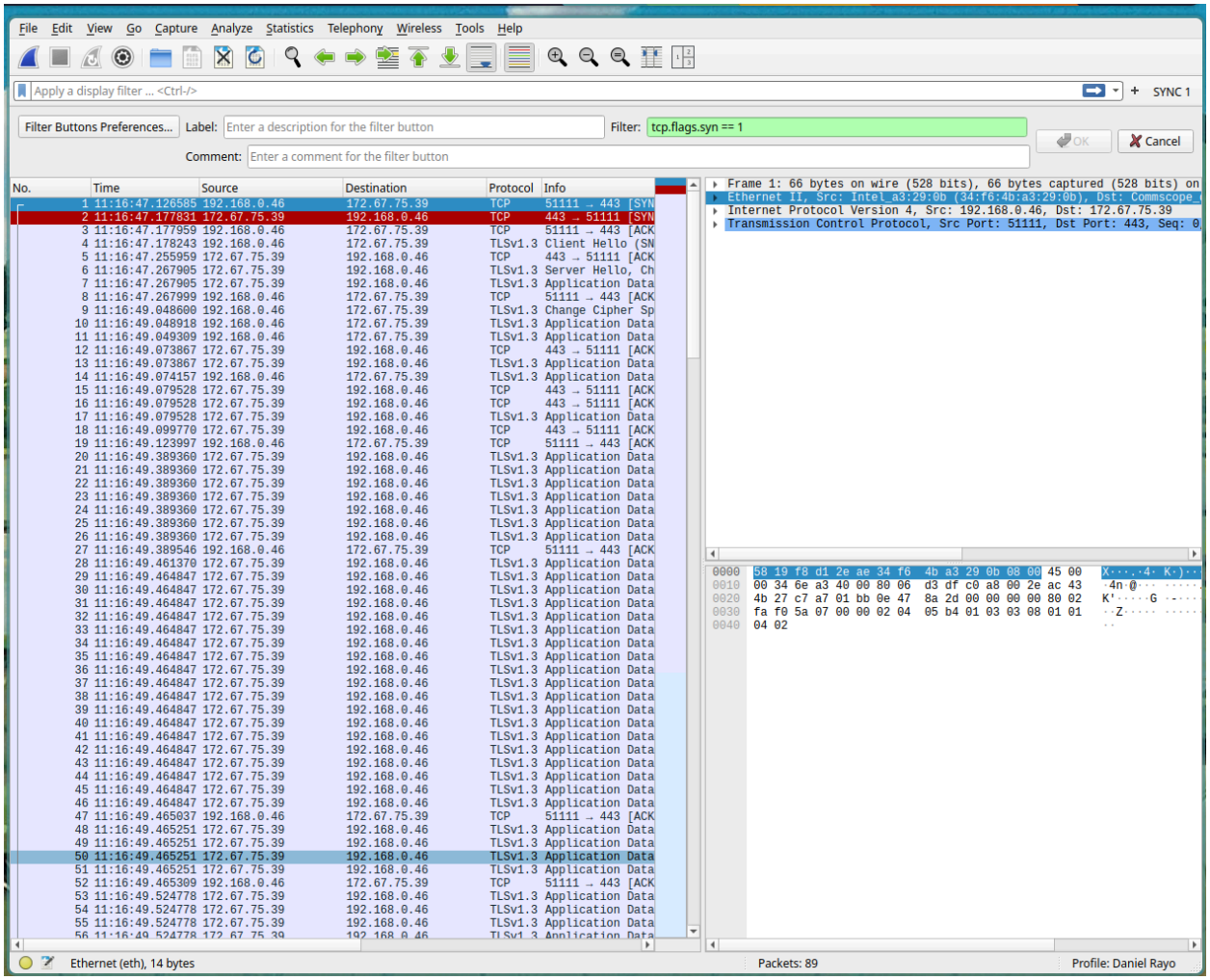
Cree un botón que aplique un filtro para paquetes TCP con la bandera SYN igual a (esquina superior derecha -> +)



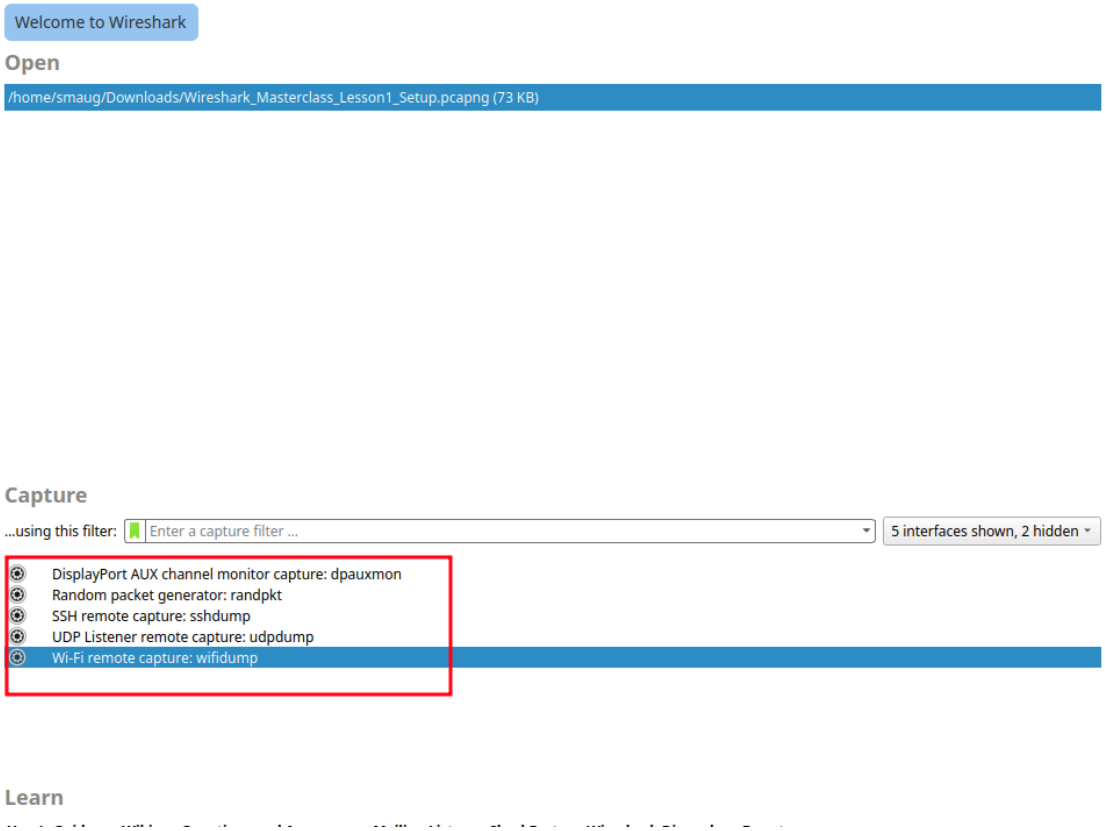
Oculte las interfaces virtuales (en caso aplique: capture -> options)



Resultado final

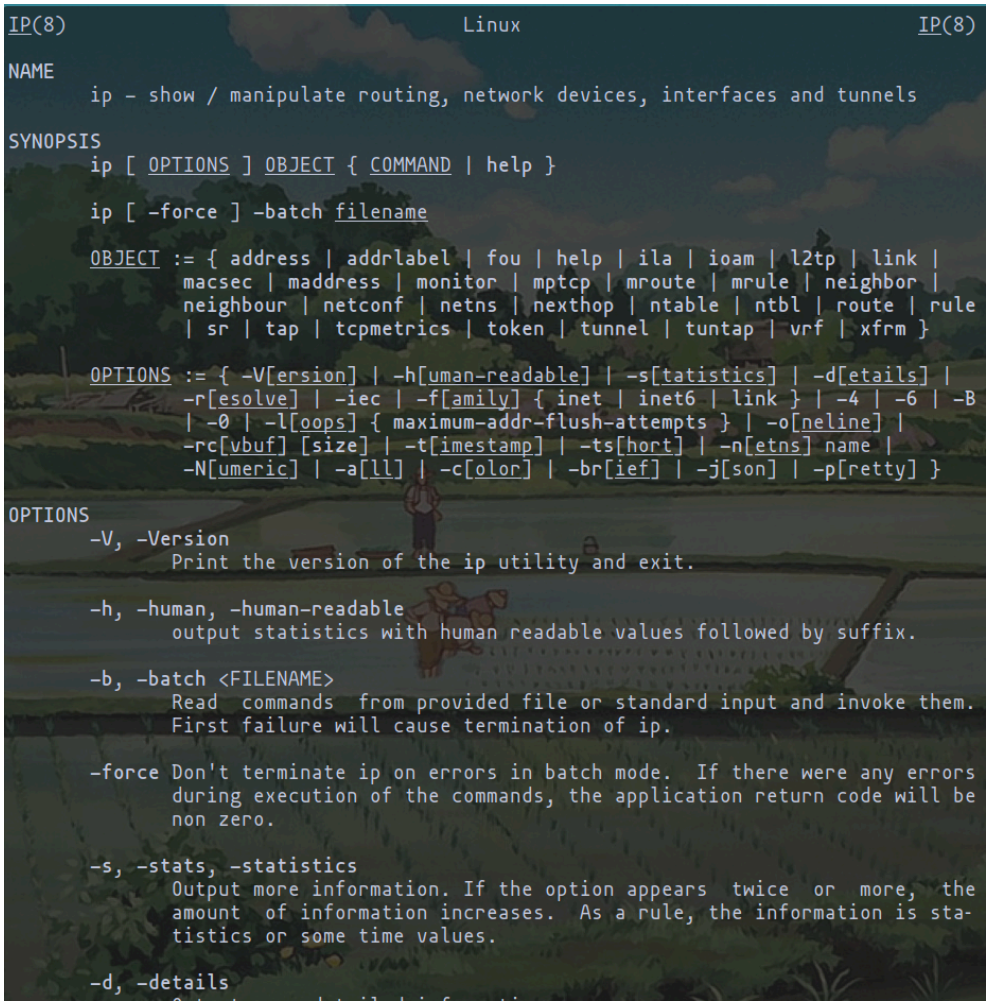


Lista de interfaces simplificada



1.2 Configuración de la captura de paquetes

1. Abra una terminal y ejecute el comando ifconfig/ipconfig (dependiendo de su OS). Detalle y explique lo observado, investigue (i.e.: ‘man ifconfig’, documentación) de ser necesario.

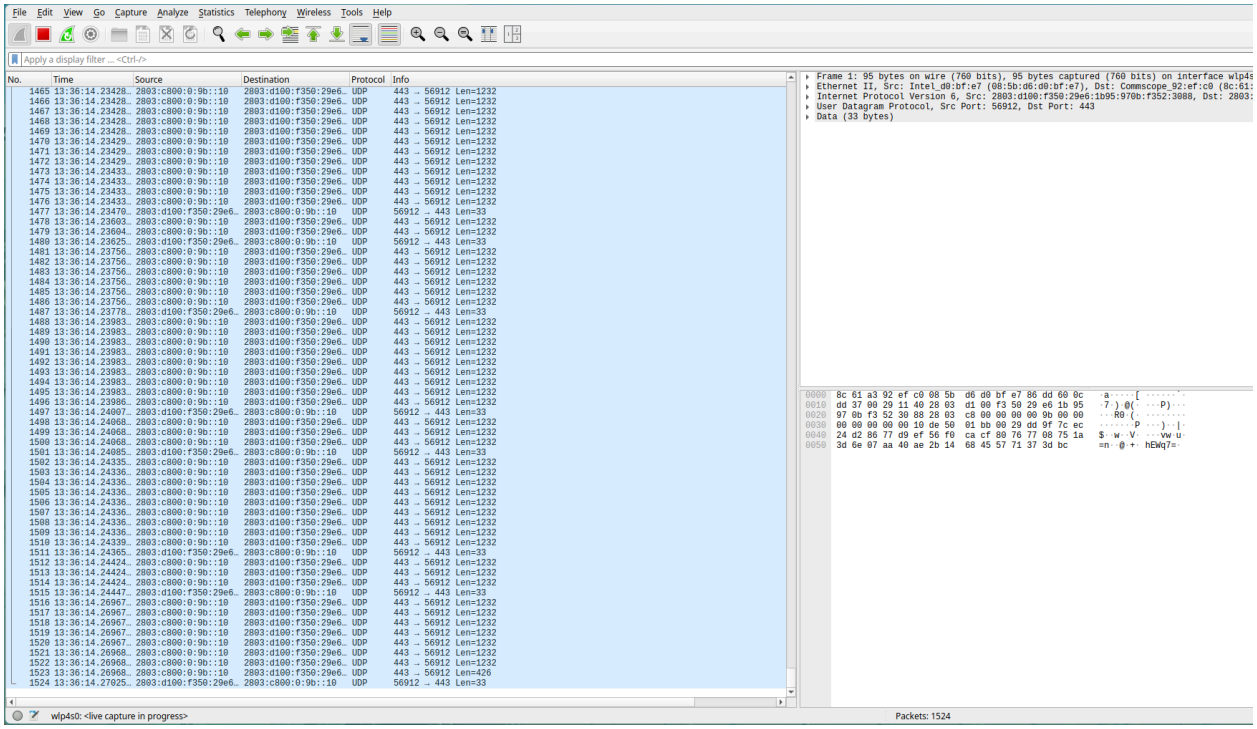


```
IP(8)                                Linux                                IP(8)

NAME
       ip - show / manipulate routing, network devices, interfaces and tunnels

SYNOPSIS
       ip [ OPTIONS ] OBJECT { COMMAND | help }

       ip [ -force ] -batch filename

       OBJECT := { address | addrlabel | fou | help | ila | ioam | l2tp | link |
                 macsec | maddress | monitor | mptcp | mroute | mrule | neighbor |
                 neighbour | netconf | netns | nexthop | ntable | ntbl | route | rule
                 | sr | tap | tcpmetrics | token | tunnel | tuntap | vrf | xfrm }

       OPTIONS := { -V[ersion] | -h[uman-readable] | -s[tatistics] | -d[etails] |
                 -r[esolve] | -iec | -f[amily] { inet | inet6 | link } | -4 | -6 | -B
                 | -0 | -l[oops] { maximum-addr-flush-attempts } | -o[neline] |
                 -rc[vbuf] [size] | -t[imestamp] | -ts[hort] | -n[etns] name |
                 -N[umeric] | -a[ll] | -c[olor] | -br[ief] | -j[son] | -p[retty] }

OPTIONS
       -V, -Version
              Print the version of the ip utility and exit.

       -h, -human, -human-readable
              output statistics with human readable values followed by suffix.

       -b, -batch <FILENAME>
              Read  commands  from provided file or standard input and invoke them.
              First failure will cause termination of ip.

       -force Don't terminate ip on errors in batch mode.  If there were any errors
              during execution of the commands, the application return code will be
              non zero.

       -s, -stats, -statistics
              Output more information. If the option appears  twice  or  more,  the
              amount  of information increases.  As a rule, the information is sta-
              tistics or some time values.

       -d, -details
```

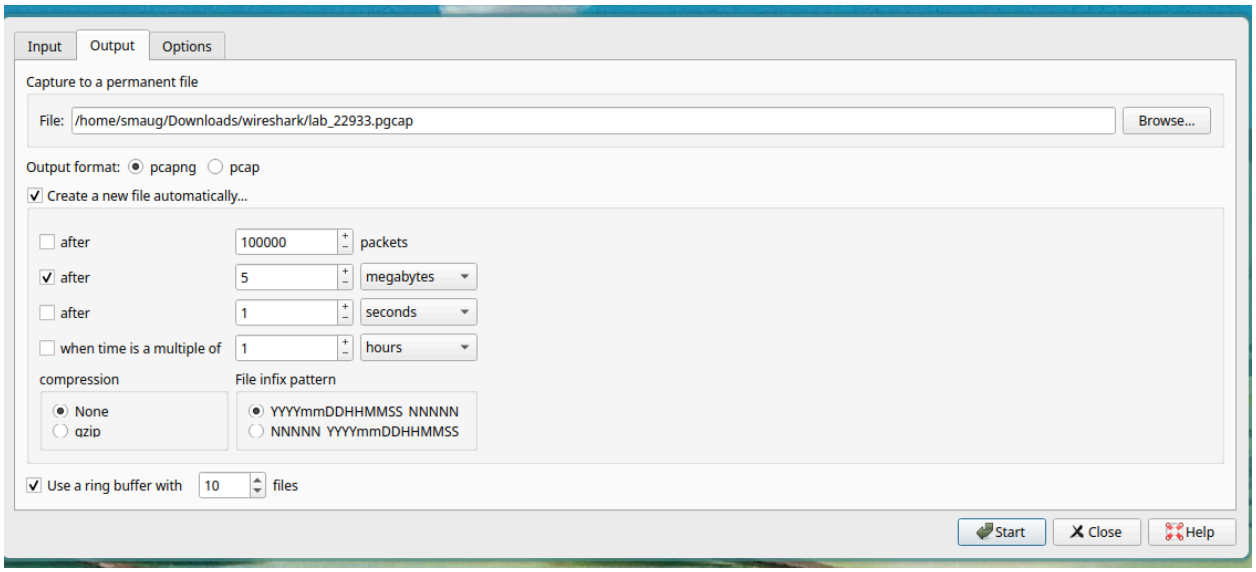
En mi caso al usar Manjaro Linux, el comando para manipular visualizar interfaces y funcionalidades de conexión se llama `ip`.

Es un comando multipropósito, que incluye muchos subcomandos cómo address, route para administrar las direcciones IP y la tabla de ruteo respectivamente.

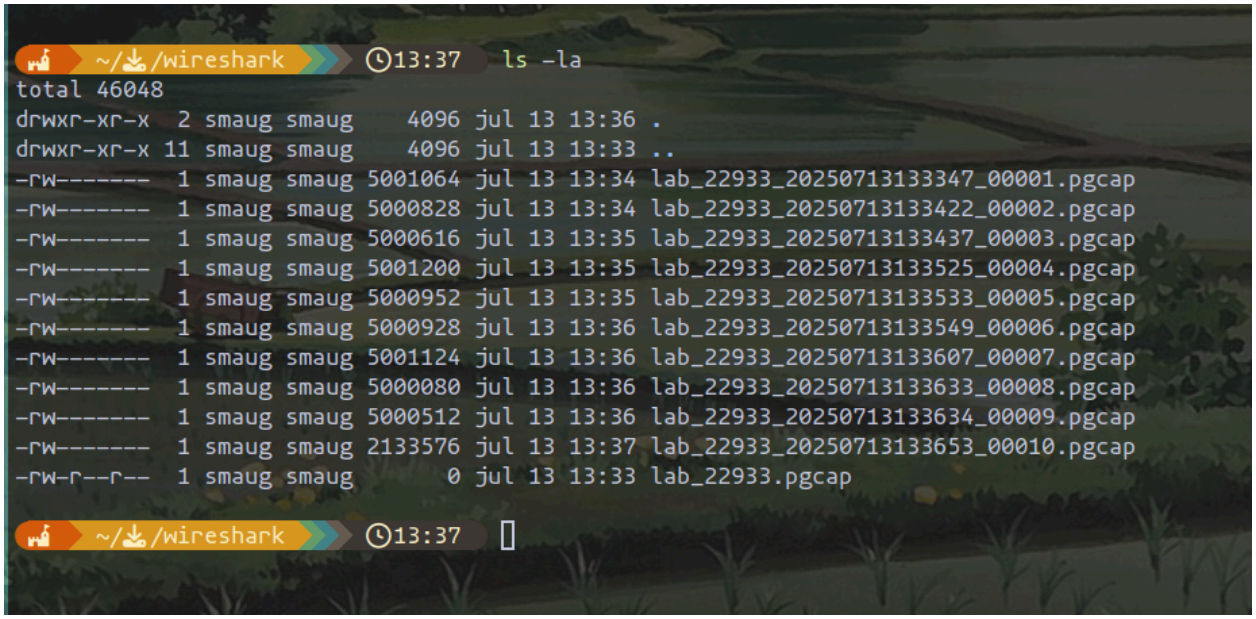
Captura de paquetes



Configuración utilizada para guardar los datos en paquetes

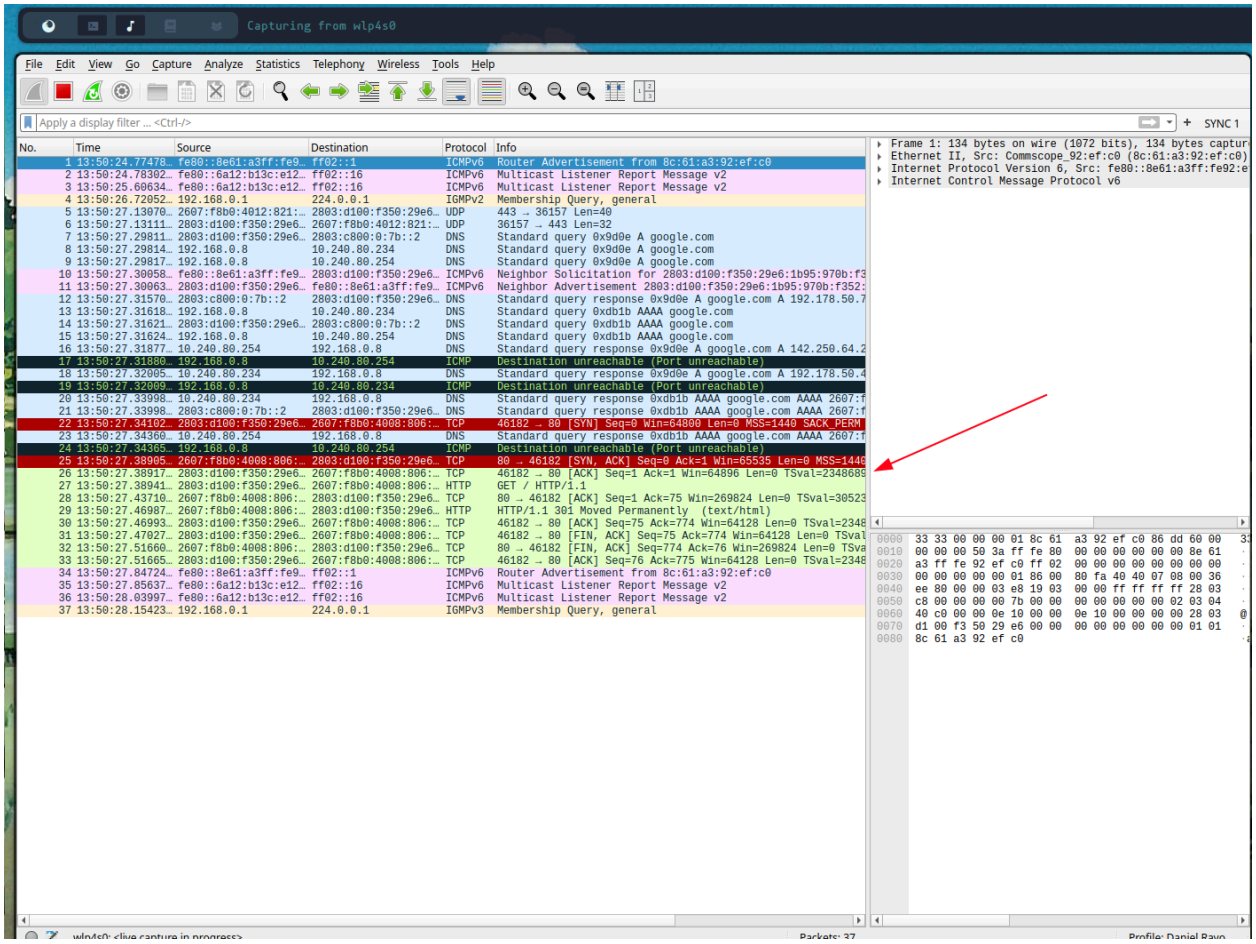


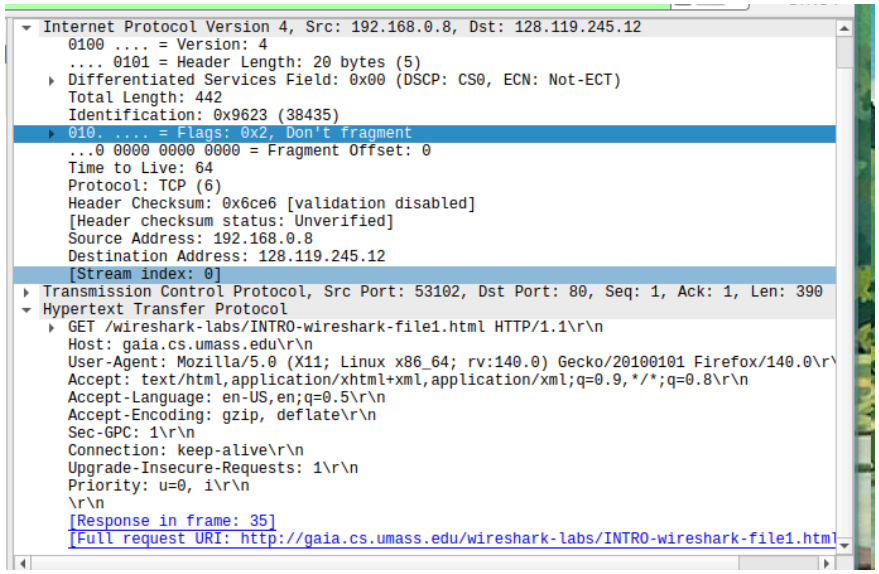
Archivos Generados por wireshark



1.3 Análisis de paquetes

Abra su navegador, inicie una captura de paquetes en Wireshark (sin filtro) en la interfaz y acceda a la siguiente direccion: http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html





a. ¿Qué versión de HTTP está ejecutando su navegador ?
   Usa la versión HTTP/1.1
b. ¿Qué versión de HTTP está ejecutando el servidor?
   Usa la versión HTTP/1.1
c. ¿Qué lenguaje (si aplica) indica el navegador que acepta el servidor?
   Indica que acepta inglés estadounidense (Accept-Language: en-US, en)

d. ¿Cuántos bytes de contenido fueron devueltos por el servidor?
   81 bytes fueron devueltos.

e. En el caso que haya un problema de rendimiento mientras se descarga la página. ¿En qué elementos de la red convendría escuchar los paquetes? ¿Es conveniente instalar Wireshark en el servidor? Justifique

Dado que fallas en transmisión de paquetes pueden ser causadas por múltiples causas, es viable monitorear las partes más importantes que participan en la conexión: el cliente, el router de la red local y el servidor objetivo.

En cuanto a si es conveniente instalar wireshark en el servidor, depende del contexto. Las ventajas de hacerlo es que permite debuggear de forma remota el tráfico en el server, tener control por medio de logs, sin embargo bajo la contra de agregar *overhead* en todas las conexiones que tenga el server además que los logs pueden a tomar bastante espacio.

Discusión

Discusión sobre la actividad, su experiencia y hallazgos. Incluir ambas partes.

Para la primera parte se pretendió crear un protocolo de comunicación utilizando solamente la comunicación verbal y oral, con la intención de poder comprender los retos a los que se enfrentan los protocolos de comunicación que implementan los sistemas de computación. En el proceso se experimentó dificultades en varios aspectos, al traducir la información a un lenguaje común (morse) para después transmitirlo por medio físicos y que la otra persona haga el proceso inverso.

Al tomar varios pasos a veces se cometieron errores en la traducción inicial, otras veces el emisor enviaba mal los caracteres, en otras ocasiones el receptor no recibía o lograba juntar todos los caracteres, y la traducción de morse era incorrecta. Este tipo de problemas son casos comunes a los que se enfrentan también los sistemas de computación.

Por otro lado, para la sección de wireshark, se descubrió el uso básico de esta herramienta para interceptar paquetes de comunicación cuando salen o entran a la computadora. El software reveló todos los detalles de diferentes capas de transporte, muchos de ellos no son intuitivos para gente no educada. Sin embargó ayudó a desvelar la gran cantidad de niveles de abstracción que se lleva para poder enviar un mensaje de un lado a otro.

Comentarios

Para poder utilizar wireshark en su máxima capacidad el conocimiento de teoría de protocolos de comunicación es indispensable, de lo contrario gran parte de la información mostrada no se encontrará relevante.

Conclusiones

- Los protocolos de comunicación son un acuerdo entre 2 partes, el incumplimiento por parte de uno de los miembros imposibilita la comunicación.
- Para la transmisión de mensajes, mientras más diferenciables los signos es estricto el protocolo más fácil es poder descubrir errores de comunicación y recepción de mensajes.
- El uso de wireshark como herramienta de debugeo monitoreo de aplicaciones puede ser útil dependiendo del contexto.

Referencias

No se utilizaron referencias externas para la elaboración de este laboratorio.