UNIVERSIDAD DE MENDOZA - FACULTAD DE INGENIERIA
SEDE SAN RAFAEL - TELEINFORMATICA - AÑO 2023
Lucas Ollarce

TRABAJO PRÁCTICO N°5

EJERCICIO N° 1

¿Qué protocolo es más seguro TCP o UDP? ¿Por qué?

Si hablamos de seguridad el protocolo TCP se considera más seguro ya que proporciona mecanismos incorporados para garantizar la entrega ordenada y confiable de los datos, por acuse de recibo, además de la detección y corrección de errores.

EJERCICIO N° 2

Si UDP es un servicio no orientado a conexión (como IP) que no es confiable, no provee mecanismos de confirmación, ni de control de congestión ¿Qué provee que no es provisto por IP?

Mientras que IP trabaja en la capa de red, UPD opera en la capa de transporte y agrega funcionalidades extras a IP como:

- **Puertos y multiplexación:** UDP utiliza puertos para permitir la comunicación de diferentes aplicaciones en un mismo dispositivo. Esto permite que varios servicios utilicen el mismo IP pero con puertos diferentes, lo que facilita la multiplexación y la entrega de datos a las aplicaciones correctas en el destino.
- **Menor sobrecarga:** UDP no tiene la sobrecarga asociada con el establecimiento y el cierre de conexiones, el seguimiento de números de secuencia, los acuses de recibo y otros mecanismos de control. Esto hace que UDP sea más eficiente en términos de uso de recursos de red y procesamiento.
- **Latencia y velocidad:** UDP puede ofrecer una menor latencia y un mayor rendimiento cuando la velocidad es prioridad. Esto lo hace adecuado para aplicaciones en tiempo real, como transmisiones de video, juegos en línea y voz sobre IP ya que no tiene los mecanismos de control de flujo y confirmación de TCP.

EJERCICIO N° 3

- Busque puertos conocidos de TCP y UDP. Anote los 8 que encuentre más relevantes.

  Puertos conocidos TCP:

  - 80: HTTP (Protocolo de transferencia de hipertexto).
  - 443: HTTPS (HTTP seguro).
  - 21: FTP (Protocolo de transferencia de archivos).
  - 25: SMTP (Protocolo simple de transferencia de correo).
  - 587: SMTP (Protocolo de transferencia de correo con autenticación).
  - 110: POP3 (Protocolo de oficina de correos, versión 3).
  - 143: IMAP (Protocolo de acceso a mensajes de Internet).
  - 22: SSH (Protocolo seguro de shell).

  Puertos conocidos UDP

  - 53: DNS (Sistema de nombres de dominio)
  - 67/68: DHCP (Protocolo de configuración dinámica de host).
  - 69: TFTP (Protocolo de transferencia de archivos trivial).
  - 123: NTP (Protocolo de tiempo de red).
  - 161/162: SNMP (Protocolo simple de administración de red).
  - 500: IPsec (Protocolo de seguridad de Internet).
  - 514: Syslog (Log del sistema operativo).
  - 4500: NAT-T (Traversing de traducción de direcciones de red).

- Busque aplicaciones y servicios de internet que funcionan sobre UDP y otras sobre TCP. Ponga algunos ejemplos y justifique por qué se usa un protocolo de transporte u otro.

  Aplicaciones que utilizan UPD:

  - **WhatsApp – Telegram:** Las aplicaciones de VoIP utilizan UDP para transmitir datos de voz en tiempo real. La prioridad en las comunicaciones de voz es minimizar la latencia y mantener una comunicación fluida. Aunque algunos paquetes pueden perderse en el camino, la comunicación de voz se mantiene en tiempo real sin la necesidad de retransmisiones.

- **Kick – Twitch:** Servicios de streaming en vivo suelen utilizar UDP para transmitir video de manera eficiente. La velocidad y la baja latencia son esenciales en las transmisiones en tiempo real, por lo que UDP se prefiere para garantizar una entrega rápida de los paquetes de video. Si se pierden algunos paquetes en el camino, el reproductor puede continuar reproduciendo el video sin interrupciones.

Aplicaciones que utilizan TCP:

- **Correo electrónico (SMTP/POP/IMAP):** Los protocolos de correo electrónico se basan en TCP. La entrega confiable de mensajes y la sincronización de los buzones de correo requieren un protocolo orientado a conexión. TCP garantiza que los correos electrónicos se entreguen correctamente y evita la pérdida de datos en el proceso de transferencia.
- **Transferencia de archivos (FTP):** TCP ofrece mecanismos de control de flujo, confirmación de paquetes y retransmisión para garantizar que los archivos se transfieran sin errores y en el orden correcto.

EJERCICIO N° 4

Un host con dirección IP 10.10.10.10 y puerto 35021 envía un paquete de 3500 bytes en capa de aplicación a la dirección IP 200.51.41.52 puerto 8080:

a. Determinar el número de segmentos UDP que se generan (indicando el formato:

cabeceras y datos), cuando se envía hacia una red Ethernet con MTU de 1500 bytes.

Source Port: 35021	Destination Port: 8080
Length	Checksum
DATA	

Para hacer esto debemos calcular el MSS (tamaño máximo de segmento) que se obtiene de restarle los bytes de la cabecera IP (20 bytes) y los bytes de la cabecera UDP (8 bytes) al MTU.

1500 – 20 – 8 = 1472 bytes

Luego se divide el tamaño del paquete por el MSS.

3500/1472 = 2,777

Y así se determina que se necesitan 3 segmentos UDP. Los primeros 2 tendrían un tamaño de 1472 bytes y el último un tamaño de 556 bytes.

b. Hacer lo mismo considerando que el nivel de transporte utilizado fuera TCP.

<table>
<tr><td colspan="3">Source Port: 35021</td><td>Source Port: 8080</td></tr>
<tr><td colspan="4">Secuence Number</td></tr>
<tr><td colspan="4">Acknowledgment</td></tr>
<tr><td>Head Length</td><td>Reserved</td><td>Flags</td><td>Window Size</td></tr>
<tr><td colspan="3">Header Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="3">Options</td><td>Padding</td></tr>
<tr><td colspan="4">DATA</td></tr>
</table>

Para hacer lo mismo utilizando TCP se le resta al MTU los bytes de la cabecera IP (20 bytes) y los bytes de la cabecera TCP (20 bytes) y obtendríamos el MSS.

$1500 – 20 – 20 = 1460$ bytes

Luego se divide el tamaño del paquete por el MSS.

3500/1460 = 2,397

Y así se determina que se necesitan 3 segmentos TCP. Los primeros 2 tendrían un tamaño de 1460 bytes y el último un tamaño de 580 bytes.

EJERCICIO N° 5

Utilice el comando netstat:

a. Ejecute en su PC el comando netstat –n. Copie el resultado y describa que información brinda.

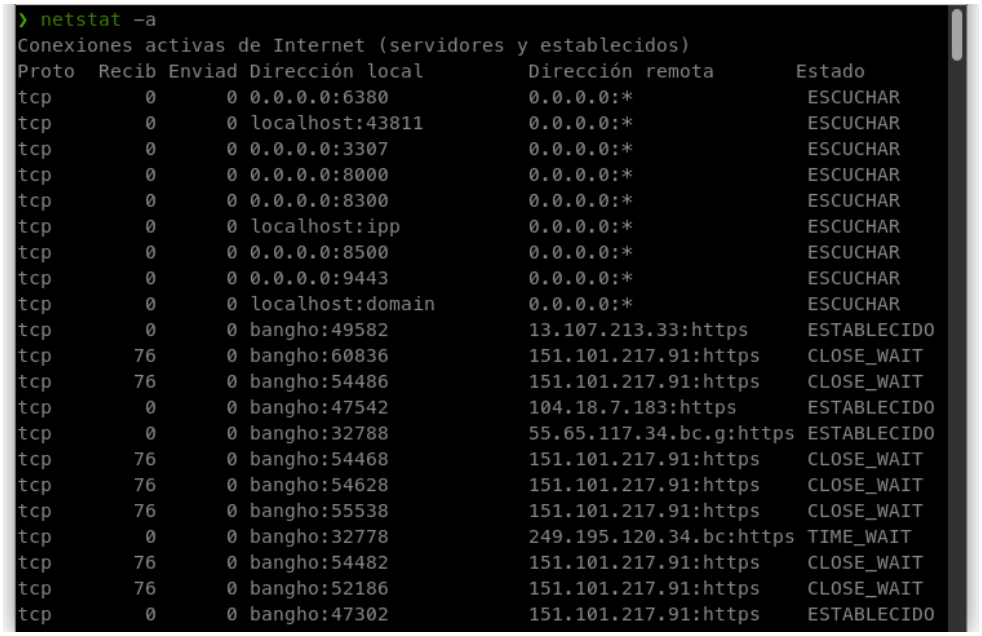
```
❯ netstat -n
Conexiones activas de Internet (servidores w/o)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 10.51.7.134:60166       104.18.2.161:443        ESTABLECIDO
tcp        0      0 10.51.7.134:39354       34.117.65.55:443        ESTABLECIDO
tcp        0      0 10.51.7.134:57744       142.251.133.36:443      ESTABLECIDO
tcp        0      0 10.51.7.134:35558       104.18.4.54:443         ESTABLECIDO
tcp        0      0 10.51.7.134:38968       142.251.133.4:443       ESTABLECIDO
tcp        0      0 10.51.7.134:41564       34.149.100.209:443      ESTABLECIDO
tcp        0      0 10.51.7.134:46024       10.51.9.72:1748         TIME_WAIT
tcp        0      0 10.51.7.134:57746       142.251.133.36:443      ESTABLECIDO
tcp        0      0 10.51.7.134:33168       35.174.127.31:443       ESTABLECIDO
tcp        0      0 10.51.7.134:34610       34.160.144.191:443      ESTABLECIDO
tcp        0      0 10.51.7.134:58262       44.211.195.229:443      ESTABLECIDO
tcp        0      0 10.51.7.134:46624       104.18.7.183:443        ESTABLECIDO
tcp        0      0 10.51.7.134:48198       142.250.79.141:443      ESTABLECIDO
tcp        0      0 10.51.7.134:56310       140.82.113.25:443       ESTABLECIDO
tcp        0      0 10.51.7.134:49996       34.237.73.95:443        ESTABLECIDO
tcp        0      0 10.51.7.134:40222       34.117.237.239:443      ESTABLECIDO
udp        0      0 10.51.7.134:68          10.51.0.2:67            ESTABLECIDO
```

La información que nos muestra el comando netstat -n es una lista de todas las conexiones de red activas en el sistema, los campos nos indican:

- **Proto:** Indica el protocolo utilizado por la conexión, que puede ser TCP o UDP.
- **Recib:** Es el número de bytes recibidos por la conexión.
- **Enviad:** Es el número de bytes enviados por la conexión.

- **Dirección local:** Indica la dirección IP y el número de puerto local.
- **Dirección remota:** Indica la dirección IP y el número de puerto remoto.
- **Estado:** Indica el estado actual de la conexión, que puede ser “ESTABLISED”, “CLOSE_WAIT” o “TIME_WAIT”.

b. Ejecute en su PC el comando netstat –a. Copie el resultado y describa que información brinda.



```
❯ netstat -a
Conexiones activas de Internet (servidores y establecidos)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 0.0.0.0:6380            0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:43811         0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:3307            0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:8000            0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:8300            0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:ipp           0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:8500            0.0.0.0:*              ESCUCHAR
tcp        0      0 0.0.0.0:9443            0.0.0.0:*              ESCUCHAR
tcp        0      0 localhost:domain        0.0.0.0:*              ESCUCHAR
tcp        0      0 bangho:49582            13.107.213.33:https    ESTABLECIDO
tcp       76      0 bangho:60836            151.101.217.91:https   CLOSE_WAIT
tcp       76      0 bangho:54486            151.101.217.91:https   CLOSE_WAIT
tcp        0      0 bangho:47542            104.18.7.183:https     ESTABLECIDO
tcp        0      0 bangho:32788            55.65.117.34.bc.g:https ESTABLECIDO
tcp       76      0 bangho:54468            151.101.217.91:https   CLOSE_WAIT
tcp       76      0 bangho:54628            151.101.217.91:https   CLOSE_WAIT
tcp       76      0 bangho:55538            151.101.217.91:https   CLOSE_WAIT
tcp        0      0 bangho:32778            249.195.120.34.bc:https TIME_WAIT
tcp       76      0 bangho:54482            151.101.217.91:https   CLOSE_WAIT
tcp       76      0 bangho:52186            151.101.217.91:https   CLOSE_WAIT
tcp        0      0 bangho:47302            151.101.217.91:https   ESTABLECIDO
```

La salida del comando netstat -a nos muestra la lista de todas la conexiones activas pero agrega los sockets que están escuchando en el sistema.

- **Proto:** Indica el protocolo utilizado por la conexión, que puede ser TCP o UDP.
- **Recib:** Es el número de bytes recibidos por la conexión.
- **Enviad:** Es el número de bytes enviados por la conexión.
- **Dirección local:** Indica la dirección IP y el número de puerto local.
- **Dirección remota:** Indica la dirección IP y el número de puerto remota.
- **Estado:** Indica el estado actual de la conexión, que puede ser “LISTEN“, “ESTABLISED”, “CLOSE_WAIT” o “TIME_WAIT”.

c. Ejecute en su PC el comando netstat –s. Copie el resultado y describa que información brinda.

```
❯ netstat -s
Ip:
    Forwarding: 1
    141927 total packets received
    4 with invalid addresses
    152 forwarded
    0 incoming packets discarded
    141363 incoming packets delivered
    72127 requests sent out
    1 fragments dropped after timeout
    7 reassemblies required
    3 packets reassembled ok
    1 packet reassemblies failed
    289 fragments received ok
    578 fragments created
Icmp:
    69 ICMP messages received
    0 input ICMP message failed
    histograma de entrada ICMP:
        destination unreachable: 63
        echo requests: 6
    75 ICMP messages sent
    0 ICMP messages failed
    histograma de salida ICMP:
        destination unreachable: 69
        echo replies: 6
IcmpMsg:
        InType3: 63
        InType8: 6
        OutType0: 6
        OutType3: 69
Tcp:
    241 active connection openings
    6 passive connection openings
    5 failed connection attempts
    18 connection resets received
    5 connections established
    137882 segments received
    68473 segments sent out
    22 segments retransmitted
    0 bad segments received
    187 resets sent
Udp:
    3562 packets received
    7 packets to unknown port received
    0 packet receive errors
    3406 packets sent
    0 receive buffer errors
    0 send buffer errors
    IgnoredMulti: 2
UdpLite:
TcpExt:
    126 TCP sockets finished time wait in fast timer
    261 delayed acks sent
    1 delayed acks further delayed because of locked socket
    Quick ack mode was activated 43 times
    9427 packet headers predicted
    1081 acknowledgments not containing data payload received
    1598 predicted acknowledgments
    TCPLostRetransmit: 2
    TCPTimeouts: 3
    TCPLossProbes: 19
    TCPDSACKOldSent: 43
    TCPDSACKRecv: 9
    58 connections reset due to unexpected data
    11 connections reset due to early user close
    TCPDSACKIgnoredNoUndo: 5
    IPReversePathFilter: 2
    TCPRcvCoalesce: 384
    TCPOFOQueue: 322
    TCPAutoCorking: 62
    TCPFromZeroWindowAdv: 4
    TCPToZeroWindowAdv: 4
    TCPWantZeroWindowAdv: 29
    TCPSynRetrans: 3
    TCPOrigDataSent: 2666
    TCPKeepAlive: 401
    TCPDelivered: 2872
    TCPAckCompressed: 120
    TcpTimeoutRehash: 3
    TCPDSACKRecvSegs: 9
IpExt:
    InMcastPkts: 620
    OutMcastPkts: 268
    InBcastPkts: 40
    OutBcastPkts: 30
    InOctets: 194230400
    OutOctets: 5372786
    InMcastOctets: 81959
    OutMcastOctets: 30007
    InBcastOctets: 11911
    OutBcastOctets: 3468
    InNoECTPkts: 142038
MPTcpExt:
```

El comando netstat -s muestra estadísticas detalladas de la red del sistema, la salida obtenida nos da información sobre los protocolos de red y sus estadísticas:

- **Ip:** Muestra estadísticas generales del protocolo IP, como el número total de paquetes enviados, recibidos, descartados, etc.
- **Icmp:** Muestra estadísticas del protocolo ICMP, incluye información sobre los mensajes ICMP enviados y recibidos.
- **Tcp:** Muestra estadísticas del protocolo TCP, incluye información sobre las conexiones TCP activas y establecidas, el número de segmentos recibidos y enviados, el número de retransmisiones, etc.
- **Udp:** Muestra estadísticas del protocolo UDP, incluye información sobre los paquetes enviados y recibidos.
- **TcpExt:** Muestra estadísticas extendidas del protocolo TCP.
- **IpExt:** Muestra estadísticas extendidas del protocolo IP.

d. Ejecute en su PC el comando netstat –r. Copie el resultado y describa que información brinda.

```
❯ netstat -r
Tabla de rutas IP del núcleo
Destino         Pasarela        Genmask         Indic   MSS Ventana irtt Interfaz
default         _gateway        0.0.0.0         UG        0 0          0 wlp2s0
link-local      0.0.0.0         255.255.0.0     U         0 0          0 docker0
172.17.0.0      0.0.0.0         255.255.0.0     U         0 0          0 docker0
172.18.0.0      0.0.0.0         255.255.0.0     U         0 0          0 br-f8cbe5a48ea5
192.168.18.0    0.0.0.0         255.255.255.0   U         0 0          0 wlp2s0
```

El comando netstat -r muestra la tabla de enrutamiento del sistema. Esta tabla contiene información sobre cómo se deben enrutar los paquetes de red a través de las rutas disponibles del sistema.

- **Destino:** La red de destino a la que se dirige el paquete.
- **Pasarela:** La dirección de gateway de la cual se debe enrutar el paquete.
- **Genmask:** La máscara de subred que se utiliza para determinar la red de destino.
- **Indic:** El índice de la interfaz de red a través de la cual se debe enrutar el paquete.
- **MSS:** El tamaño máximo de segmento que se puede enviar a través de la ruta.
- **Ventana:** El tamaño de la ventana de recepción que se puede utilizar a través de la ruta.
- **Irtt:** El tiempo de retardo inicial que se debe utilizar a través de la ruta.
- **Interfaz:** La interfaz de red a través de la cual se debe enrutar el paquete.

EJERCICIO N° 6

Utilice le comando netstat.

a. De acuerdo a la información del ejercicio anterior cierre todas las conexiones externas a su PC, y desconéctese de la red. Espere unos minutos para que se cierren todas las conexiones abiertas.

b. Desde la consola de Linux ejecute el comando clear.

c. Ejecute en su pc el comando netstat –n. Copie el resultado.

```
❯ netstat -n
Conexiones activas de Internet (servidores w/o)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp       76      0 192.168.18.4:60836      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:54486      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:54468      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:54628      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:55538      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:54482      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:52186      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:47302      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:49410      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:49420      151.101.217.91:443     CLOSE_WAIT
```

d. Conectese de nuevo a la red.

e. Ejecute el comando netstat –n. Copie el resultado.

```
❯ netstat -n
Conexiones activas de Internet (servidores w/o)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp       76      0 192.168.18.4:60836      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:54486      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:42916      13.227.83.99:80         TIME_WAIT
tcp       76      0 192.168.18.4:54468      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:54628      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:55538      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:54482      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:52186      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:47302      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:49410      151.101.217.91:443      CLOSE_WAIT
tcp       76      0 192.168.18.4:49420      151.101.217.91:443      CLOSE_WAIT
tcp6       0      0 192.168.18.4:1716       192.168.18.147:59402    ESTABLECIDO
udp        0      0 192.168.18.4:34969      15.237.97.214:123       ESTABLECIDO
udp        0      0 192.168.18.4:60807      170.155.148.1:123       ESTABLECIDO
udp        0      0 192.168.18.4:36491      52.10.183.132:123       ESTABLECIDO
udp        0      0 192.168.18.4:68         192.168.18.1:67         ESTABLECIDO
```

f. Abra una página de Internet.

g. Ejecute el comando netstat –n. Copie el resultado.

```
❯ netstat -n
Conexiones activas de Internet (servidores w/o)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 192.168.18.4:50140      34.117.65.55:443        ESTABLECIDO
tcp       76      0 192.168.18.4:60836      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:35906      192.124.249.22:80       ESTABLECIDO
tcp       76      0 192.168.18.4:54486      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:49822      185.199.110.153:443     ESTABLECIDO
tcp        0      0 192.168.18.4:53472      18.232.254.126:443      ESTABLECIDO
tcp        0      0 192.168.18.4:58064      172.217.173.227:80      ESTABLECIDO
tcp        0      0 192.168.18.4:55390      13.227.93.190:80        ESTABLECIDO
tcp       76      0 192.168.18.4:54468      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:57468      34.160.144.191:443      ESTABLECIDO
tcp        0      0 192.168.18.4:54304      200.51.41.139:443       TIME_WAIT
tcp       76      0 192.168.18.4:54628      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:54854      192.16.49.85:80         ESTABLECIDO
tcp        0      0 192.168.18.4:35960      184.31.2.16:80          ESTABLECIDO
tcp       76      0 192.168.18.4:55538      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:50146      34.117.65.55:443        ESTABLECIDO
tcp        0      0 192.168.18.4:55094      34.107.221.82:80        ESTABLECIDO
tcp        0      0 192.168.18.4:57228      172.217.173.228:443     ESTABLECIDO
tcp        0      0 192.168.18.4:52288      34.117.237.239:443      ESTABLECIDO
tcp       76      0 192.168.18.4:54482      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:35972      184.31.2.16:80          TIME_WAIT
tcp        0      0 192.168.18.4:54346      200.51.41.139:443       TIME_WAIT
tcp       76      0 192.168.18.4:52186      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:54862      192.16.49.85:80         ESTABLECIDO
tcp        0      0 192.168.18.4:54842      192.16.49.85:80         ESTABLECIDO
tcp        0      0 192.168.18.4:46334      104.26.0.89:443         ESTABLECIDO
tcp        0      0 192.168.18.4:36364      54.188.114.15:443       TIME_WAIT
tcp        0      0 192.168.18.4:59596      34.120.208.123:443      ESTABLECIDO
tcp        0      0 192.168.18.4:54450      34.149.100.209:443      ESTABLECIDO
tcp       76      0 192.168.18.4:47302      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:58062      172.217.173.227:80      ESTABLECIDO
tcp       76      0 192.168.18.4:49410      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:48294      142.251.133.74:443      TIME_WAIT
tcp       76      0 192.168.18.4:49420      151.101.217.91:443      CLOSE_WAIT
tcp        0      0 192.168.18.4:55110      34.107.221.82:80        ESTABLECIDO
tcp6       0      0 192.168.18.4:1716       192.168.18.147:59402    ESTABLECIDO
udp        0      0 192.168.18.4:68         192.168.18.1:67         ESTABLECIDO
```

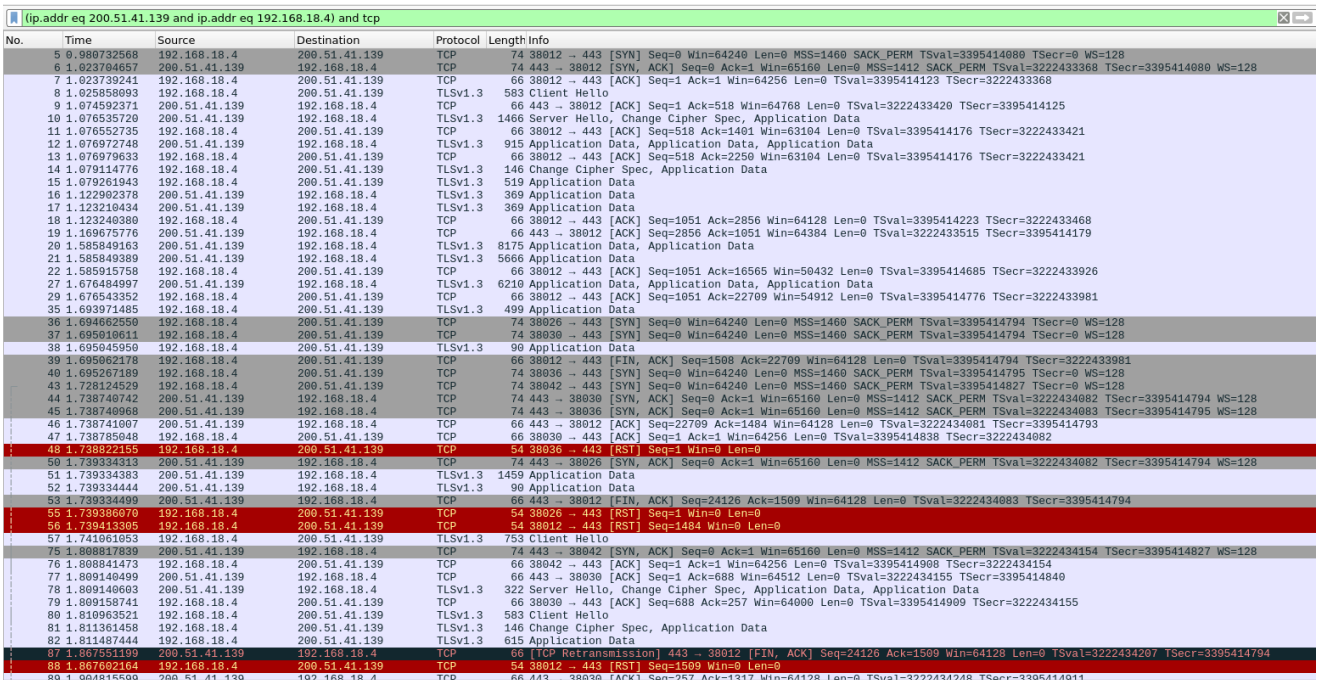
h. Vea su correo.

i. Ejecute el comand netstat –n. Copie el resultado.

```
❯ netstat -n
Conexiones activas de Internet (servidores w/o)
Proto  Recib Enviad Dirección local         Dirección remota       Estado
tcp        0      0 192.168.18.4:50140      34.117.65.55:443       ESTABLECIDO
tcp        0      0 192.168.18.4:45018      142.250.79.110:443     TIME_WAIT
tcp        0      0 192.168.18.4:45842      142.250.79.110:443     TIME_WAIT
tcp       76      0 192.168.18.4:60836      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:54486      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:49822      185.199.110.153:443    ESTABLECIDO
tcp        0      0 192.168.18.4:46864      172.217.173.227:80     ESTABLECIDO
tcp        0      0 192.168.18.4:53472      18.232.254.126:443     ESTABLECIDO
tcp        0      0 192.168.18.4:48912      142.251.133.37:443     ESTABLECIDO
tcp        0      0 192.168.18.4:46880      172.217.173.227:80     ESTABLECIDO
tcp        0      0 192.168.18.4:48456      142.251.133.42:443     TIME_WAIT
tcp        0      0 192.168.18.4:58064      172.217.173.227:80     ESTABLECIDO
tcp        0      0 192.168.18.4:38952      142.251.134.46:443     TIME_WAIT
tcp        0      0 192.168.18.4:55390      13.227.93.190:80       TIME_WAIT
tcp       76      0 192.168.18.4:54468      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:57468      34.160.144.191:443     ESTABLECIDO
tcp        0      0 192.168.18.4:56606      18.67.0.13:80          TIME_WAIT
tcp        0      0 192.168.18.4:39270      142.251.133.202:443    TIME_WAIT
tcp        0      0 192.168.18.4:39476      172.217.172.109:443    TIME_WAIT
tcp       76      0 192.168.18.4:54628      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:38962      142.251.134.46:443     TIME_WAIT
tcp        0      0 192.168.18.4:54854      192.16.49.85:80        TIME_WAIT
tcp        0      0 192.168.18.4:35960      184.31.2.16:80         TIME_WAIT
tcp        0   3834 192.168.18.4:52222      142.251.133.69:443     ESTABLECIDO
tcp        0      0 192.168.18.4:36434      142.251.134.14:443     TIME_WAIT
tcp       76      0 192.168.18.4:55538      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:47850      18.67.0.13:80          TIME_WAIT
tcp        0      0 192.168.18.4:50146      34.117.65.55:443       ESTABLECIDO
tcp        0      0 192.168.18.4:51472      172.217.173.228:443    TIME_WAIT
tcp        0      0 192.168.18.4:48864      172.67.71.39:443       TIME_WAIT
tcp        0      0 192.168.18.4:55094      34.107.221.82:80       ESTABLECIDO
tcp        0      0 192.168.18.4:57228      172.217.173.228:443    TIME_WAIT
tcp        0      0 192.168.18.4:52288      34.117.237.239:443     ESTABLECIDO
tcp        0      0 192.168.18.4:48442      142.251.133.42:443     ESTABLECIDO
tcp       76      0 192.168.18.4:54482      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:49068      172.67.71.39:443       TIME_WAIT
tcp        0      0 192.168.18.4:45356      13.227.83.125:443      TIME_WAIT
tcp        0      0 192.168.18.4:33158      142.251.133.10:443     TIME_WAIT
tcp        0      0 192.168.18.4:43140      13.82.67.141:80        TIME_WAIT
tcp       76      0 192.168.18.4:52186      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:54862      192.16.49.85:80        TIME_WAIT
tcp        0      0 192.168.18.4:54842      192.16.49.85:80        TIME_WAIT
tcp        0      0 192.168.18.4:39258      142.251.133.202:443    ESTABLECIDO
tcp        0      0 192.168.18.4:59672      13.90.21.104:80        TIME_WAIT
tcp        0      0 192.168.18.4:34324      142.251.134.42:443     TIME_WAIT
tcp        0      0 192.168.18.4:46334      104.26.0.89:443        ESTABLECIDO
tcp        0      0 192.168.18.4:49348      142.251.133.35:443     TIME_WAIT
tcp        0      0 192.168.18.4:38084      13.227.83.125:443      TIME_WAIT
tcp        0      0 192.168.18.4:59596      34.120.208.123:443     ESTABLECIDO
tcp        0      0 192.168.18.4:41070      142.251.134.3:443      TIME_WAIT
tcp        0      0 192.168.18.4:54450      34.149.100.209:443     ESTABLECIDO
tcp       76      0 192.168.18.4:47302      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:33142      142.251.133.10:443     ESTABLECIDO
tcp        0      0 192.168.18.4:58062      172.217.173.227:80     TIME_WAIT
tcp       76      0 192.168.18.4:49410      151.101.217.91:443     CLOSE_WAIT
tcp       76      0 192.168.18.4:49420      151.101.217.91:443     CLOSE_WAIT
tcp        0      0 192.168.18.4:49406      142.251.133.206:443    TIME_WAIT
tcp        0      0 192.168.18.4:55110      34.107.221.82:80       ESTABLECIDO
tcp        0      0 192.168.18.4:39778      142.250.79.97:443      TIME_WAIT
tcp        0      0 192.168.18.4:47660      142.251.133.195:443    TIME_WAIT
tcp6       0      0 192.168.18.4:1716       192.168.18.147:59402   ESTABLECIDO
udp        0      0 127.0.0.1:51299         127.0.0.53:53          ESTABLECIDO
udp        0      0 192.168.18.4:68         192.168.18.1:67        ESTABLECIDO
udp        0    768 192.168.18.4:41423      192.168.18.1:53        ESTABLECIDO
udp        0    768 192.168.18.4:53845      192.168.18.1:53        ESTABLECIDO
```

EJERCICIO N° 7

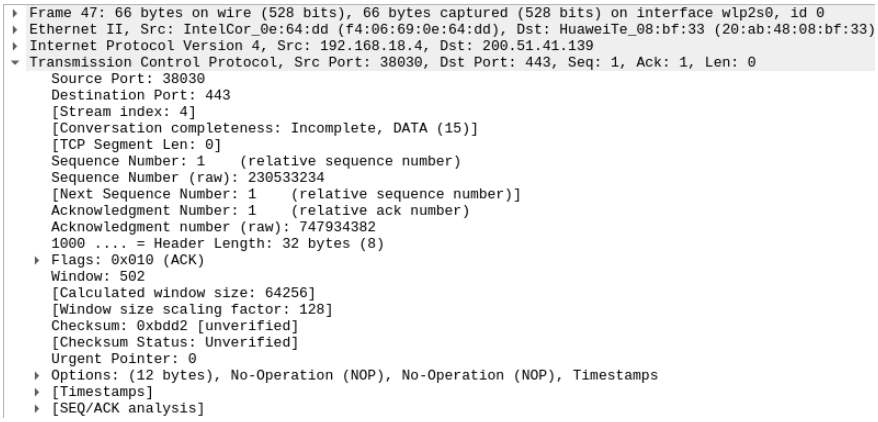
a. Abra el programa wireshark, entre a la página de la UM y luego muestre los paquetes de saludo inicial asociados a esta consulta. (syn – syn ack – ack).



(ip.addr eq 200.51.41.139 and ip.addr eq 192.168.18.4) and tcp

No.	Time	Source	Destination	Protocol	Length	Info
5	0.980732568	192.168.18.4	200.51.41.139	TCP	74	38012 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414080 TSecr=0 WS=128
6	1.023704657	200.51.41.139	192.168.18.4	TCP	74	443 → 38012 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222433368 TSecr=3395414080 WS=128
7	1.023739241	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3395414123 TSecr=3222433368
8	1.025858093	192.168.18.4	200.51.41.139	TLSv1.3	583	Client Hello
9	1.074592371	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3222433420 TSecr=3395414125
10	1.076535720	200.51.41.139	192.168.18.4	TLSv1.3	1466	Server Hello, Change Cipher Spec, Application Data
11	1.076552735	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=518 Ack=1401 Win=63104 Len=0 TSval=3395414176 TSecr=3222433421
12	1.076972748	200.51.41.139	192.168.18.4	TLSv1.3	915	Application Data, Application Data, Application Data
13	1.076979633	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=518 Ack=2250 Win=63104 Len=0 TSval=3395414176 TSecr=3222433421
14	1.079114776	192.168.18.4	200.51.41.139	TLSv1.3	146	Change Cipher Spec, Application Data
15	1.079261943	192.168.18.4	200.51.41.139	TLSv1.3	519	Application Data
16	1.122902378	200.51.41.139	192.168.18.4	TLSv1.3	369	Application Data
17	1.123210434	200.51.41.139	192.168.18.4	TLSv1.3	369	Application Data
18	1.123240380	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=1051 Ack=2856 Win=64128 Len=0 TSval=3395414223 TSecr=3222433468
19	1.169675776	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [ACK] Seq=2856 Ack=1051 Win=64384 Len=0 TSval=3222433515 TSecr=3395414179
20	1.585849163	200.51.41.139	192.168.18.4	TLSv1.3	8175	Application Data, Application Data
21	1.585849389	200.51.41.139	192.168.18.4	TLSv1.3	5666	Application Data
22	1.585915758	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=1051 Ack=16565 Win=50432 Len=0 TSval=3395414685 TSecr=3222433926
27	1.676484997	200.51.41.139	192.168.18.4	TLSv1.3	6210	Application Data, Application Data, Application Data
29	1.676543352	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [ACK] Seq=1051 Ack=22709 Win=54912 Len=0 TSval=3395414776 TSecr=3222433981
35	1.693971485	192.168.18.4	200.51.41.139	TLSv1.3	499	Application Data
36	1.694662550	192.168.18.4	200.51.41.139	TCP	74	38026 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414794 TSecr=0 WS=128
37	1.695010611	192.168.18.4	200.51.41.139	TCP	74	38030 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414794 TSecr=0 WS=128
38	1.695045950	192.168.18.4	200.51.41.139	TLSv1.3	90	Application Data
39	1.695062178	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [FIN, ACK] Seq=1508 Ack=22709 Win=64128 Len=0 TSval=3395414794 TSecr=3222433981
40	1.695267189	192.168.18.4	200.51.41.139	TCP	74	38036 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414795 TSecr=0 WS=128
43	1.728124529	192.168.18.4	200.51.41.139	TCP	74	38042 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414827 TSecr=0 WS=128
44	1.738740742	200.51.41.139	192.168.18.4	TCP	74	443 → 38030 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434082 TSecr=3395414794 WS=128
45	1.738740968	200.51.41.139	192.168.18.4	TCP	74	443 → 38036 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434083 TSecr=3395414795 WS=128
46	1.738741007	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [ACK] Seq=22709 Ack=1484 Win=64128 Len=0 TSval=3222434081 TSecr=3395414793
47	1.738785048	192.168.18.4	200.51.41.139	TCP	66	38030 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3395414838 TSecr=3222434082
48	1.738822155	192.168.18.4	200.51.41.139	TCP	54	38036 → 443 [RST] Seq=1 Win=0 Len=0
50	1.739334313	200.51.41.139	192.168.18.4	TCP	74	443 → 38026 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434082 TSecr=3395414794 WS=128
51	1.739334383	200.51.41.139	192.168.18.4	TLSv1.3	1459	Application Data
52	1.739334444	200.51.41.139	192.168.18.4	TLSv1.3	90	Application Data
53	1.739334499	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [FIN, ACK] Seq=24126 Ack=1509 Win=64128 Len=0 TSval=3222434083 TSecr=3395414794
55	1.739386070	192.168.18.4	200.51.41.139	TCP	54	38026 → 443 [RST] Seq=1 Win=0 Len=0
56	1.739413305	192.168.18.4	200.51.41.139	TCP	54	38012 → 443 [RST] Seq=1484 Win=0 Len=0
57	1.741061053	192.168.18.4	200.51.41.139	TLSv1.3	753	Client Hello
75	1.808817839	200.51.41.139	192.168.18.4	TCP	74	443 → 38042 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434154 TSecr=3395414827 WS=128
76	1.808841473	192.168.18.4	200.51.41.139	TCP	66	38042 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3395414908 TSecr=3222434154
77	1.809140499	200.51.41.139	192.168.18.4	TCP	66	443 → 38030 [ACK] Seq=1 Ack=688 Win=64512 Len=0 TSval=3222434155 TSecr=3395414840
78	1.809140603	200.51.41.139	192.168.18.4	TLSv1.3	322	Server Hello, Change Cipher Spec, Application Data, Application Data
79	1.809158741	192.168.18.4	200.51.41.139	TCP	66	38030 → 443 [ACK] Seq=688 Ack=257 Win=64000 Len=0 TSval=3395414909 TSecr=3222434155
80	1.810963521	192.168.18.4	200.51.41.139	TLSv1.3	583	Client Hello
81	1.811361458	192.168.18.4	200.51.41.139	TLSv1.3	146	Change Cipher Spec, Application Data
82	1.811487444	192.168.18.4	200.51.41.139	TLSv1.3	615	Application Data
87	1.867551199	200.51.41.139	192.168.18.4	TCP	66	[TCP Retransmission] 443 → 38012 [FIN, ACK] Seq=24126 Ack=1509 Win=64128 Len=0 TSval=3222434207 TSecr=3395414794
88	1.867602164	192.168.18.4	200.51.41.139	TCP	54	38012 → 443 [RST] Seq=1509 Win=0 Len=0
89	1.904815599	200.51.41.139	192.168.18.4	TCP	66	443 → 38030 [ACK] Seq=257 Ack=1317 Win=64128 Len=0 TSval=3222434248 TSecr=3395414911

b. Explique la cabecera TCP y su valores.

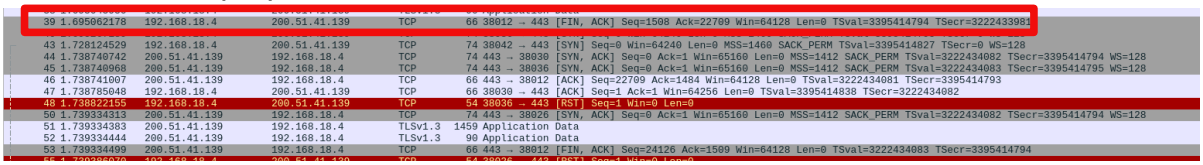


```
▸ Frame 47: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface wlp2s0, id 0
▸ Ethernet II, Src: IntelCor_0e:64:dd (f4:06:69:0e:64:dd), Dst: HuaweiTe_08:bf:33 (20:ab:48:08:bf:33)
▸ Internet Protocol Version 4, Src: 192.168.18.4, Dst: 200.51.41.139
▾ Transmission Control Protocol, Src Port: 38030, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
    Source Port: 38030
    Destination Port: 443
    [Stream index: 4]
    [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 230533234
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 747934382
    1000 .... = Header Length: 32 bytes (8)
  ▸ Flags: 0x010 (ACK)
    Window: 502
    [Calculated window size: 64256]
    [Window size scaling factor: 128]
    Checksum: 0xbdd2 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  ▸ [Timestamps]
  ▸ [SEQ/ACK analysis]
```

- **Source Port (Puerto origen):** Es el número de puerto del emisor del paquete TCP. El puerto origen es 38030.
- **Destination Port (Puerto destino):** Es el número de puerto del receptor del paquete TCP. El puerto destino es 443, que es el protocolo HTTPS.
- **Sequence Number (Número de secuencia):** Es un número de secuencia de 23 bits que indica el orden de los bytes en un flujo de datos TCP. El número de secuencia inicial es 1.

- **Acknowledgment Number (Número de acuse de recibo):** Es un numero de acuse de recibo de 32 bits que indica el siguiente byte esperado por el receptor. El número de acuse de recibo es 1.
- **Header Length (Longitud de cabecera):** Indica la longitud de la cabecera TCP en múltiplos de 4 bytes. La longitud de la cabecera es de 32 bytes.
- **Flags (Banderas):** Son indicadores de control utilizados en la cabecera TCP. El valor 0x010 indica que se establecio el bit de ACK, significa que el receptor ha confirmado que recibió los datos anteriores.
- **Window (Ventana):** Es el tamaño de la ventana de recepción del receptor en bytes. La ventana tiene un tamaño de 502.
- **Checksum (Suma de verificación):** Es un valor de comprobación utilizado para detectar errores en la cabecera TCP y los datos. El valor 0xbdd2 indica la suma de verificación del paquete, pero no se ha verificado su validez.
- **Urgent Pointer (Puntero Urgente):** Se utiliza para indicar datos urgentes presentes en el segmento TCP, El puntero urgente es 0, significa que no hay datos urgentes en el segmento.
- **Options (Opciones):** Son campos adicionales utilizados para proporcionar funcionalidades adicionales en la cabecera TCP. Se incluyen 12 bytes de opciones que contiene 2 operaciones sin acción (NOP) y las marcas de tiempo (Timestamps).

c. Muestre los paquetes de cierre de conexión.

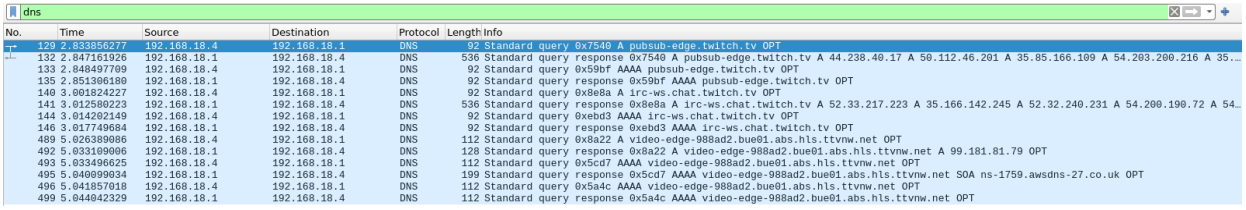


39	1.695062178	192.168.18.4	200.51.41.139	TCP	66	38012 → 443 [FIN, ACK] Seq=1508 Ack=22709 Win=64128 Len=0 TSval=3395414794 TSecr=3222433981
43	1.728124529	192.168.18.4	200.51.41.139	TCP	74	38042 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3395414827 TSecr=0 WS=128
44	1.738740742	200.51.41.139	192.168.18.4	TCP	74	443 → 38030 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434082 TSecr=3395414794 WS=128
45	1.738740968	200.51.41.139	192.168.18.4	TCP	74	443 → 38036 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434083 TSecr=3395414795 WS=128
46	1.738741007	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [ACK] Seq=22709 Ack=1484 Win=64128 Len=0 TSval=3222434081 TSecr=3395414793
47	1.738785048	192.168.18.4	200.51.41.139	TCP	66	38030 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3395414838 TSecr=3222434082
48	1.738822155	192.168.18.4	200.51.41.139	TCP	54	38036 → 443 [RST] Seq=1 Win=0 Len=0
50	1.739334313	200.51.41.139	192.168.18.4	TCP	74	443 → 38026 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1412 SACK_PERM TSval=3222434082 TSecr=3395414794 WS=128
51	1.739334383	200.51.41.139	192.168.18.4	TLSv1.3	1459	Application Data
52	1.739334444	200.51.41.139	192.168.18.4	TLSv1.3	90	Application Data
53	1.739334499	200.51.41.139	192.168.18.4	TCP	66	443 → 38012 [FIN, ACK] Seq=24126 Ack=1509 Win=64128 Len=0 TSval=3222434083 TSecr=3395414794

Como se puede observar en rojo el servidor de la UM envía el paquete TCP para el cierre de conexión con la flag [FIN, ACK]

EJERCICIO N° 8

a. Abra el programa wireshark, entre a cualquier página y luego muestre los paquetes UDP que están asociados. (DNS utiliza UDP para realizar sus consultas).

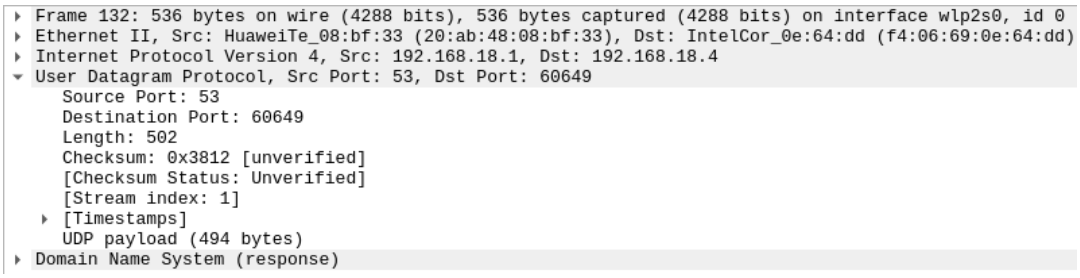


dns

No.	Time	Source	Destination	Protocol	Length	Info
129	2.833856277	192.168.18.4	192.168.18.1	DNS	92	Standard query 0x7540 A pubsub-edge.twitch.tv OPT
132	2.847161926	192.168.18.1	192.168.18.4	DNS	536	Standard query response 0x7540 A pubsub-edge.twitch.tv A 44.238.40.17 A 50.112.46.201 A 35.85.166.109 A 54.203.200.216 A 35.…
133	2.848497709	192.168.18.4	192.168.18.1	DNS	92	Standard query 0x59bf AAAA pubsub-edge.twitch.tv OPT
135	2.851306180	192.168.18.1	192.168.18.4	DNS	92	Standard query response 0x59bf AAAA pubsub-edge.twitch.tv OPT
140	3.001824227	192.168.18.4	192.168.18.1	DNS	92	Standard query 0x8e8a A irc-ws.chat.twitch.tv OPT
141	3.012580223	192.168.18.1	192.168.18.4	DNS	536	Standard query response 0x8e8a A irc-ws.chat.twitch.tv A 52.33.217.223 A 35.166.142.245 A 52.32.240.231 A 54.200.190.72 A 54…
144	3.014202149	192.168.18.4	192.168.18.1	DNS	92	Standard query 0xebd3 AAAA irc-ws.chat.twitch.tv OPT
146	3.017749684	192.168.18.1	192.168.18.4	DNS	92	Standard query response 0xebd3 AAAA irc-ws.chat.twitch.tv OPT
489	5.026389086	192.168.18.4	192.168.18.1	DNS	112	Standard query 0x8a22 A video-edge-988ad2.bue01.abs.hls.ttvnw.net OPT
492	5.033109006	192.168.18.1	192.168.18.4	DNS	128	Standard query response 0x8a22 A video-edge-988ad2.bue01.abs.hls.ttvnw.net A 99.181.81.79 OPT
493	5.033496625	192.168.18.4	192.168.18.1	DNS	112	Standard query 0x5cd7 AAAA video-edge-988ad2.bue01.abs.hls.ttvnw.net OPT
495	5.040099034	192.168.18.1	192.168.18.4	DNS	199	Standard query response 0x5cd7 AAAA video-edge-988ad2.bue01.abs.hls.ttvnw.net SOA ns-1759.awsdns-27.co.uk OPT
496	5.041857018	192.168.18.4	192.168.18.1	DNS	112	Standard query 0x5a4c AAAA video-edge-988ad2.bue01.abs.hls.ttvnw.net OPT
499	5.044042329	192.168.18.1	192.168.18.4	DNS	112	Standard query response 0x5a4c AAAA video-edge-988ad2.bue01.abs.hls.ttvnw.net OPT

En la captura se observan los paquetes UPD de las consultas DNS enviadas y recibidas para acceder a la página de twitch.tv

b. Explique la cabecera UDP y su valores.

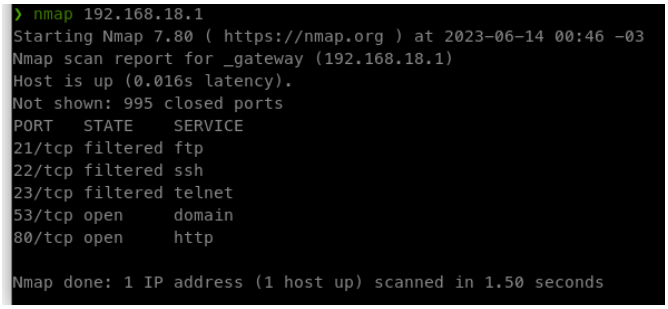


- **Source port (Puerto origen):** Es el número de puerto del emisor del paquete UDP. El puerto origen es 53, que es utilizado para el servicio DNS.
- **Destination port (Puerto destino):** Es el número de puerto del receptor del paquete UDP. El puerto destino es 60649.
- **Length (Longitud):** Indica la longitud total del paquete UDP (incluye cabecera y datos). La longitud es de 502 bytes.
- **Checksum (Suma de verificación):** Es un valor de comprobación utilizado para detectar errores en la cabecera UDP y los datos. El valor 0x3812 indica la suma de verificación del paquete, pero no se ha verificado su validez.
- **Stream index (Índice de flujo):** Es un indicador utilizado para identificar un flujo especifico de datos en una comunicación. El índice asignado al paquete UDP es 1.
- **Timestamps (Marcas de tiempo):** Indica que se incluyen marcas de tiempo en la cabecera UDP. Las marcas de tiempo se utilizan para registrar el momento en que se generó o recibió un paquete.
- **UDP payload (Carga útil UDP):** Se refiere a los datos reales que se transmiten a través del protocolo UDP. La carga útil tiene un tamaño de 494 bytes.

EJERCICIO N° 9

Abra el programa nmap y realice los siguientes escaneos:

a. A la dirección IP de su puerta de enlace.



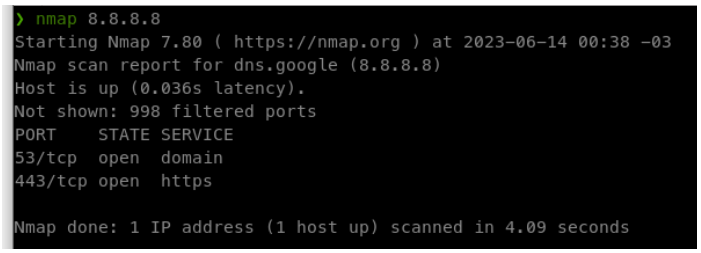
En el escaneo realizado a la puerta de enlace y el host esta activo, o sea que está en línea y responde las solicitudes con una latencia de 0.022 segundos.

En el análisis de puertos se encuentran 995 puertos cerrado y se identificaron 5 puertos (3 filtrados y 2 abiertos):

- El puerto 21: En este puerto filtrado indica que el servicio FTP no es accesible desde el exterior.
- El puerto 22: En este puerto filtrado indica que el servicio SSH no es accesible desde el exterior.
- El puerto 23: En este puerto filtrado indica que el servicio Telnet no es accesible desde el exterior.
- El puerto 53: En este puerto abierto esta disponible el servicio DNS que se utiliza para las consultas y respuestas de DNS.
- El puerto 80: En este puerto abierto esta disponible el servicio HTTP que es el protocolo utilizado para acceder a sitios web no cifrados.

b. A la dirección IP 8.8.8.8

En el escaneo realizado a la dirección 8.8.8.8 se ve que la IP pertenece a un



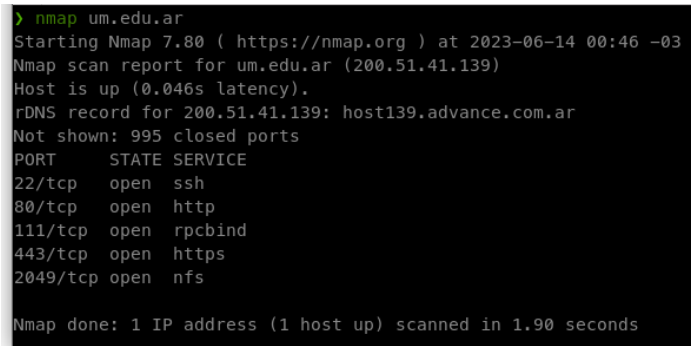
servidor DNS de Google y el host esta activo, o sea que está en línea y responde las solicitudes con una latencia de 0.036 segundos.

En el análisis de puertos se encuentran 998 puertos filtrados, y se identificaron 2 puertos abiertos:

- El puerto 53: En este puerto abierto esta disponible el servicio DNS que se utiliza para las consultas y respuestas de DNS.
- El puerto 443: En este puerto esta disponible el servicio HTTPS que es una versión segura del protocolo HTTP que tiene cifrado para proteger las comunicaciones.

c. A la dirección um.edu.ar

En el escaneo realizado a la dirección um.edu.ar se ve que 200.51.41.139 es la IP

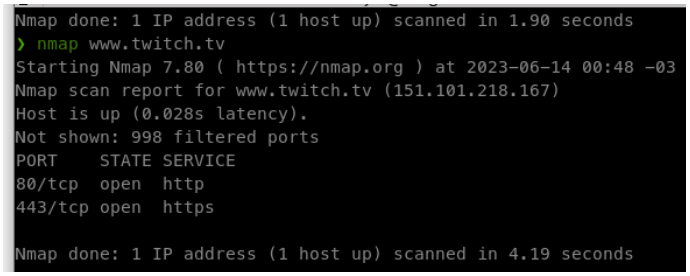


asociada y el host esta activo, o sea que está en línea y responde a las solicitudes con una latencia de 0.046 segundos.

En el análisis de puertos se encuentran 995 puertos cerrados, y se identificaron 5 puertos abiertos:

- El puerto 22: En este puerto esta disponible el servicio SSH que es un protocolo para acceder de forma segura a sistemas remota.
- El puerto 80: En este puerto esta disponible el servicio HTTP que es el protocolo utilizado para acceder a sitios web no cifrados.
- El puerto 111: En este puerto esta disponible el servicio RPCBIND
- El puerto 443: En este puerto esta disponible el servicio HTTPS que es una versión segura del protocolo HTTP que tiene cifrado para proteger las comunicaciones.
- El puerto 2049: En este puerto esta disponible el servicio NFS que es un protocolo utilizado para compartir archivos y carpetas en una red.

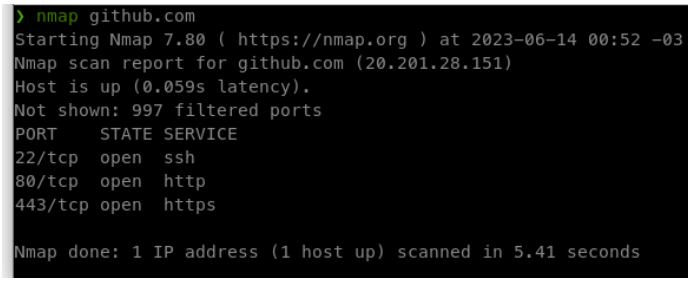
d. A dos direcciones públicas de Internet (puede ser IP o dominio).



En el escaneo realizado a la dirección www.twitch.tv se ve que 151.101.218.167 es la IP asociada y el host esta activo, o sea que está en línea y responde a las solicitudes con una latencia de 0.028 segundos.

En el análisis de puertos se encuentran 998 puertos cerrados, y se identificaron 2 puertos abiertos:

- El puerto 80: En este puerto esta disponible el servicio HTTP que es el protocolo utilizado para acceder a sitios web no cifrados.
- El puerto 443: En este puerto esta disponible el servicio HTTPS que es una versión segura del protocolo HTTP que tiene cifrado para proteger las comunicaciones.



En el escaneo realizado a la dirección github.com se ve que 20.201.28.151 es la IP asociada y el host esta activo, o sea que está en línea y responde a las solicitudes con una latencia de 0.059 segundos.

En el análisis de puertos se encuentran 997 puertos cerrados, y se identificaron 3 puertos abiertos:

- El puerto 22: En este puerto esta disponible el servicio SSH que es un protocolo para acceder de forma segura a sistemas remota.
- El puerto 80: En este puerto esta disponible el servicio HTTP que es el protocolo utilizado para acceder a sitios web no cifrados.
- El puerto 443: En este puerto esta disponible el servicio HTTPS que es una versión segura del protocolo HTTP que tiene cifrado para proteger las comunicaciones.

e. Indique en cada caso la información recibida.