TALLER 1 WIRESHARK SALUDO 3 VIAS

UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

LUIS MIGUEL POLO – 20182020158

NICOLÁS DAVID SABOGAL – 20202020008

LUIS SEBASTIAN MARTINEZ GUERRERO - 20191005153

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

INGENIERÍA DE SISTEMAS

REDES DE COMUNICACIONES III

PAULO ALONSO GAONA GARCIA

2024-III

INTRODUCCIÓN

Wireshark es el analizador de paquetes más conocido y utilizado en todo el mundo. Gracias a este programa, podremos capturar y analizar en detalle todo el tráfico de red que entra y sale de nuestro computador.

OBJETIVOS

- Familiarizarse con el analizador de protocolos utilizado en el laboratorio de Redes.
- Analizar tráfico Unicast, multicast y broadcast.
- Analizar tráfico en todos los niveles del modelo de comunicación OSI.
- Identificar saludo de tres vías en un proceso de comunicación.

DESARROLLO

PARTE I

En una red de área local (casa, laboratorio, etc), correr la aplicación de wireshark y definir tres escenarios de trabajo a saber: i) acceso a correo electrónico universidad y/o personal, ii) acceso una plataforma red social, iii) acceso plataforma de comercio electrónico.

A partir de estos escenarios realizar:

1. Detallar el formato de una dirección Unicast, Broadcast y Multicast (si aplica).
2. Identificar por lo menos 3 MAC y 3 direcciones IP asociadas en el proceso.
3. Describir formato trama SMTP, POP3, TCP, TLSV, conexiones HTTPs, según sea el caso.
4. Realizar un diagrama completo de acceso a cada servicio (proceso de encapsulamiento) e identificar saludo de tres vías en cada caso.
5. Describir la ruta (saltos, equipos y direcciones) identificadas dentro del proceso de comunicación para cada caso.

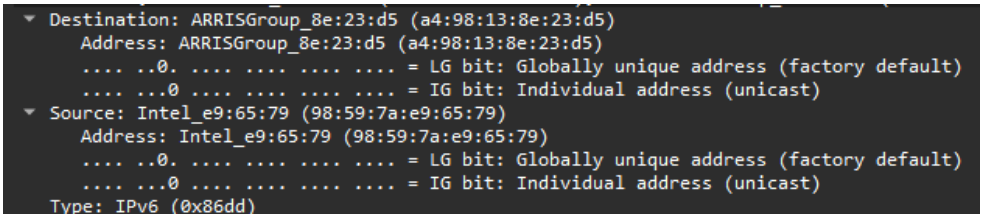
Para cada acceso responder:

- ¿Cuál es el número de puerto de origen de TCP?
- ¿Cómo clasificaría el puerto de origen?
- ¿Cuál es el número del puerto de destino de TCP?

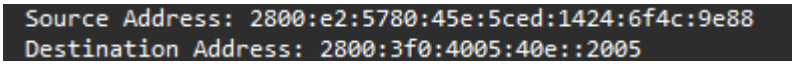
- ¿Cómo clasificaría el puerto de destino?
- ¿Qué marcadores están establecidos?
- ¿Qué número de secuencia relativo está establecido?

i) Acceso a correo electrónico personal

1. Las direcciones del destinatario y la fuente pertenecen a redes de tipo unicast.

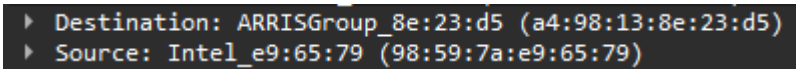


2. Direcciones IPv6 asociadas:



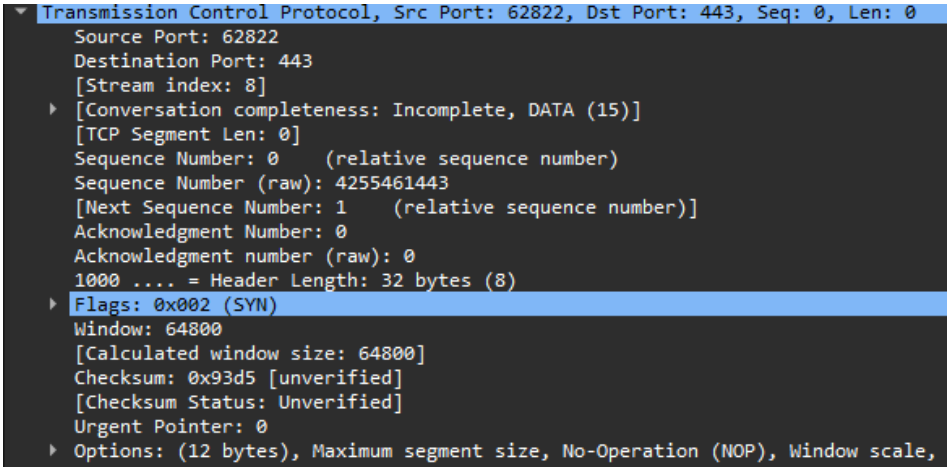
   - Host: 2800:e2:5780:45e:5ced:1424:6f4c:9e88
   - Gmail: 2800:3f0:4005:410::2005

Direcciones MAC asociadas:



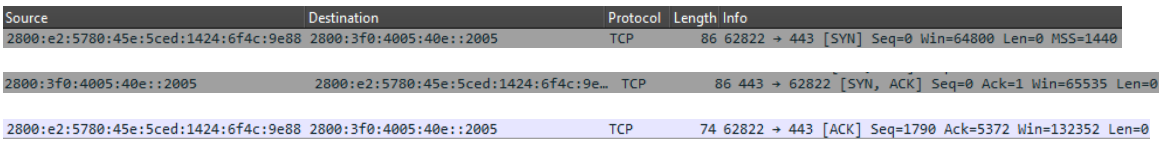
   - Host: 98-59-7A-E9-65-79
   - Gmail: a4-98-13-8e-23-d5

3. Descripción de trama TCP en wireshark:



Nombre	Bits	Descripción	Valor
Source Port	16	Identifica el terminal de origen.	62822
Destination Port	16	Identifica el terminal de destino.	443
Sequence Number	32	Identifica el primer byte de datos.	0
ACK Number	32	Contiene el valor del próximo byte que está dispuesto a recibir.	0
Header Length	4	Longitud de cabecera para identificar el inicio de los datos.	32 bytes
Window	16	Cuantos bits componen la ventana de transmisión.	64800
Checksum	16	Se utiliza para detectar errores.	0x93d5
Urgent Pointer	16	Sirve para indicar si los datos son urgentes.	0
TCP Options		Permite añadir campos a la cabecera.	

4. En el siguiente esquema se puede identificar las tramas que componen el saludo 3 vías.



El proceso comienza con un paquete SYN enviado desde el cliente (puerto 62822) al servidor (puerto 443), indicando la intención de iniciar una conexión. El servidor responde con un paquete SYN, ACK, confirmando la recepción del SYN y enviando su propio número de secuencia. Finalmente, el cliente envía un paquete ACK de vuelta al servidor, confirmando la recepción del SYN, ACK del servidor. Con este intercambio, la conexión TCP queda establecida, y las partes están listas para comenzar a intercambiar datos.

```
▾ Ethernet II, Src: Intel_e9:65:79 (98:59:7a:e9:65:79), Dst: ARRISGroup_8e:23:d5 (a4:98:13:8e:23:d5)
  ▸ Destination: ARRISGroup_8e:23:d5 (a4:98:13:8e:23:d5)
  ▸ Source: Intel_e9:65:79 (98:59:7a:e9:65:79)
    Type: IPv6 (0x86dd)
▾ Internet Protocol Version 6, Src: 2800:e2:5780:45e:5ced:1424:6f4c:9e88, Dst: 2800:3f0:4005:40e::2005
    0110 .... = Version: 6
  ▸ .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0101 1000 0110 0000 1110 = Flow Label: 0x5860e
    Payload Length: 20
    Next Header: TCP (6)
    Hop Limit: 64
    Source Address: 2800:e2:5780:45e:5ced:1424:6f4c:9e88
    Destination Address: 2800:3f0:4005:40e::2005
▸ Transmission Control Protocol, Src Port: 62822, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

5. Traza de ruta hacia la dirección IPv6 de destino:

```
C:\Users\PC-LUISMIGUEL>tracert 2800:3f0:4005:410::2005

Traza a 2800:3f0:4005:410::2005 sobre caminos de 30 saltos como máximo.

  1     3 ms     4 ms     4 ms  2800:e2:5780:45e:a698:13ff:fe8e:23d5
  2     *        *        *     Tiempo de espera agotado para esta solicitud.
  3    12 ms    15 ms    15 ms  2800:e0::10:cb1e:15
  4    11 ms    12 ms    12 ms  2800:e0::10:cb1e:14
  5    13 ms    12 ms    17 ms  2001:4860:1:1::147a
  6    13 ms    23 ms    12 ms  2800:3f0:804b::1
  7    12 ms    12 ms    12 ms  2001:4860:0:1::4d8e
  8    14 ms    13 ms    15 ms  2001:4860:0:1::3552
  9    14 ms     *       15 ms  2001:4860:0:1::881f
 10    14 ms    11 ms    14 ms  2001:4860:0:1::77a5
 11    11 ms    12 ms    10 ms  2800:3f0:4005:410::2005

Traza completa.
```

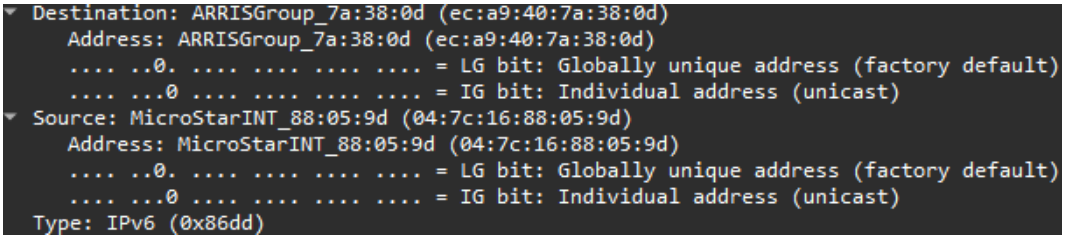
La traza muestra que el paquete recorre 11 saltos para llegar a su destino. Las direcciones IPV6 de los saltos 3 y 4 corresponden al proveedor de servicios de internet (EPM telecomunicaciones), mientras que las demás direcciones corresponden a Google, el cual es quien administra Gmail.

Preguntas:

a. El puerto de origen es 443
b. El puerto 443 es un puerto utilizado para el protocolo HTTPS, el cual permite la comunicación segura en la web.
c. El puerto de destino es 62822
d. El marcador establecido es 0x002 que es SYN
e. El número de secuencia relativo es 0

ii) Acceso a una plataforma de red social (Instagram)

1. WireShark detecta automáticamente el tipo de red que es el destinatario y la fuente, en el caso de nuestro host e Instagram son direcciones unicast.



2. Algunas direcciones IP y MAC asociadas al proceso son:
   Direcciones IPv6:
   - Host: 2800:484:27c:1030:185:7bf4:b4d6:c020

     `Destination Address: 2800:484:27c:1030:185:7bf4:b4d6:c020`
   - Instagram: 2a03:2880:f32f:c0:face:b00c:0:43fe

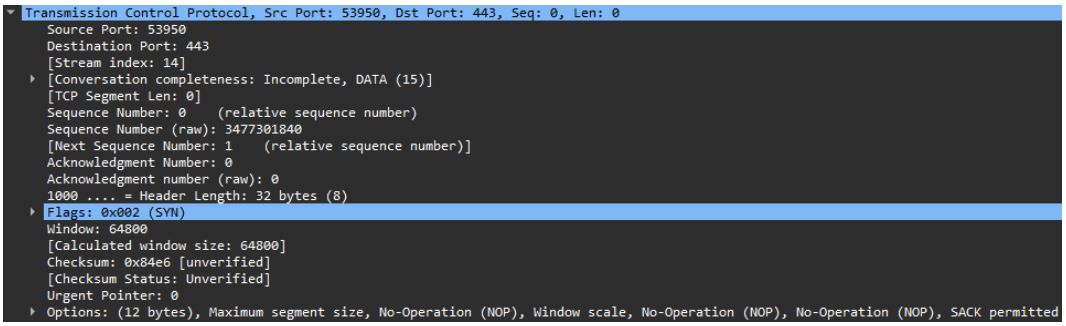
     `Source Address: 2a03:2880:f32f:c0:face:b00c:0:43fe`

   Direcciones MAC:
   - Host: 04-7C-16-88-05-9D

     `MicroStarINT_88:05:9d (04:7c:16:88:05:9d)`
   - Instagram: EC-A9-40-7A-38-0D

     `ARRISGroup 7a:38:0d (ec:a9:40:7a:38:0d)`

3. En nuestro caso, el protocolo usado es el TCP, y WireShark lo describe de la siguiente manera, en la primera trama respecto al saludo 3 vías.

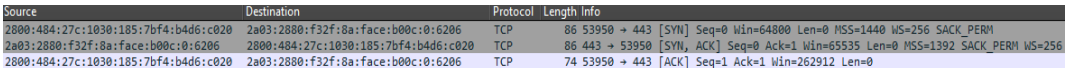


   Donde los componentes están descritos por:

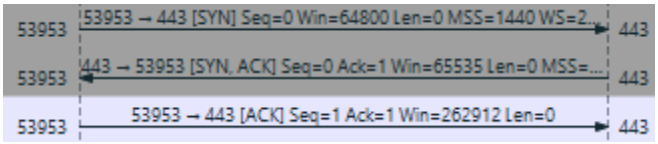
Nombre	Bits	Descripción	Valor
Source Port	16	Identifica el terminal de origen.	53950
Destination Port	16	Identifica el terminal de destino.	443
Sequence Number	32	Identifica el primer byte de datos.	0
ACK Number	32	Contiene el valor del próximo byte que está dispuesto a recibir.	0
Header Length	4	Longitud de cabecera para identificar el inicio de los datos.	32 bytes
Window	16	Cuantos bits componen la ventana de transmisión.	64800
Checksum	16	Se utiliza para detectar errores.	0x84e6

Urgent Pointer	16	Sirve para indicar si los datos son urgentes.	0
TCP Options		Permite añadir campos a la cabecera.	

4. A partir del análisis de trafico de WireShark, tenemos las siguientes tramas que permiten ver el saludo de 3 vías.



Donde la gráfica de flujo, entre las dos IPs es el siguiente:



5. Usamos la línea de comandos, para trazar la ruta que tenemos al ingresar a esa dirección ipv6, dando lo siguiente:

```
C:\Users\iamse>tracert 2a03:2880:f32f:c0:face:b00c:0:43fe

Traza a la dirección instagram-p36-shv-02-bog2.fbcdn.net [2a03:2880:f32f:c0:face:b00c:0:43fe]
sobre un máximo de 30 saltos:

  1     2 ms     2 ms     2 ms  2800:484:27c:1030:eea9:40ff:fe7a:380d
  2    24 ms    24 ms    16 ms  2800:485:0:18::1
  3    18 ms    23 ms    24 ms  2800:483:100:1::1
  4    26 ms    10 ms     8 ms  peer-as14080.pr02.bog1.tfbnw.net [2620:0:1cff:dead:beee::b5f]
  5    21 ms    19 ms    28 ms  ae20.pr02.bog1.tfbnw.net [2620:0:1cff:dead:beee::b5e]
  6    21 ms    24 ms    19 ms  po222.asw02.bog2.tfbnw.net [2620:0:1cff:dead:beef::37dc]
  7    22 ms    22 ms    15 ms  po237.psw01.bog2.tfbnw.net [2620:0:1cff:dead:beef::9357]
  8    22 ms    21 ms    21 ms  be5.msw1ab.02.bog2.tfbnw.net [2a03:2880:f0aa:ffff::2d3]
  9    19 ms    18 ms    20 ms  instagram-p36-shv-02-bog2.fbcdn.net [2a03:2880:f32f:c0:face:b00c:0:43fe]
```

Las primeras tres direcciones, son direcciones entre el host y el proveedor de servicios de internet, las otras direcciones que vemos son propiamente del servicio de Meta, empresa que hostea diferentes redes sociales incluyendo Instagram.

Preguntas:

- El puerto origen es 53953.
- No está reservado para ningún uso definido, es un puerto privado del cliente.
- El puerto destino es 443.
- El puerto 443 está reservado para https, es un puerto bien conocido en el servidor.
- El marcador establecido es 0x002 que es SYN
- El número de secuencia relativo es 0.

iii) Acceso a una plataforma de comercio electrónico

1. En este caso, la red usa únicamente el protocolo IPv4. La máscara de red es 255.255.255.0, que corresponde a un sufijo /24, lo que indica que las direcciones están compuestas en los primeros 3 octantes están reservados para la dirección de red 192.168.0.0 y el último octante determina: la dirección del host en direcciones unicast para 1-254 y la dirección broadcast para 255. Bajo este protocolo no corresponden direcciones multicast.

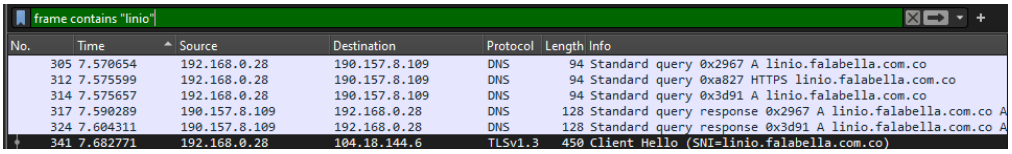
```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . : fe80::6d40:5321:53d4:69cc%4
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.28
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
```

2. Algunas direcciones IP y MAC asociadas al proceso son:

   Direcciones IP:

   - Host: 192.168.0.28
   - Gateway: 192.168.0.1
   - DNS Telmex Bogotá: 190.157.8.109
   - Página web de Falabella (Linio): 104.18.144.6



   Direcciones MAC:

   - Adaptador Wi-Fi: 34-6F-24-A8-16-FB

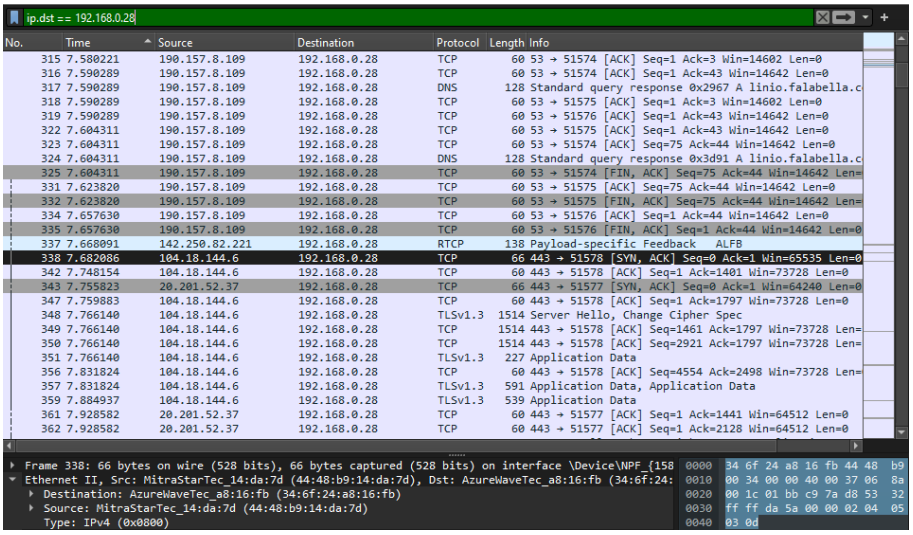
```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Descripción . . . . . . . . . . . . . . . : Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
   Dirección física. . . . . . . . . . . . . : 34-6F-24-A8-16-FB
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local. . . : fe80::6d40:5321:53d4:69cc%4(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.28(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : viernes, 16 de agosto de 2024 9:30:05 a. m.
   La concesión expira . . . . . . . . . . . : lunes, 26 de agosto de 2024 9:32:35 a. m.
   Puerta de enlace predeterminada . . . . . : 192.168.0.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 70545188
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2A-BC-F4-83-34-6F-24-A8-16-FB
   Servidores DNS. . . . . . . . . . . . . . : 190.157.8.109
                                       190.157.8.101
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

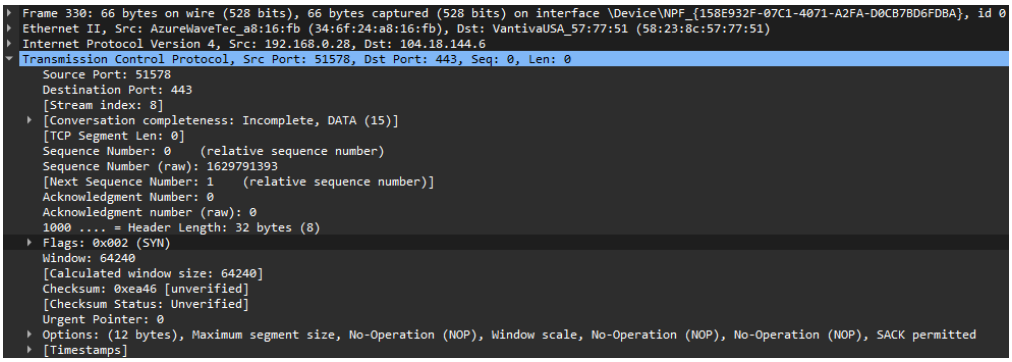
   - Gateway del enrutador: 58-24-8C-57-77-51

```
Interfaz: 192.168.0.28 ---- 0x4
  Dirección de Internet          Dirección física      Tipo
  192.168.0.1           58-23-8c-57-77-51     dinámico
  192.168.0.31          14-bb-6e-03-71-b5     dinámico
  192.168.0.255         ff-ff-ff-ff-ff-ff     estático
  224.0.0.2             01-00-5e-00-00-02     estático
  224.0.0.22            01-00-5e-00-00-16     estático
  224.0.0.251           01-00-5e-00-00-fb     estático
  224.0.0.252           01-00-5e-00-00-fc     estático
  239.255.255.177       01-00-5e-7f-ff-b1     estático
  239.255.255.246       01-00-5e-7f-ff-f6     estático
  239.255.255.250       01-00-5e-7f-ff-fa     estático
  255.255.255.255       ff-ff-ff-ff-ff-ff     estático
```

- Interfaz de respuesta del servicio: 44-48-B9-14-DA-7D



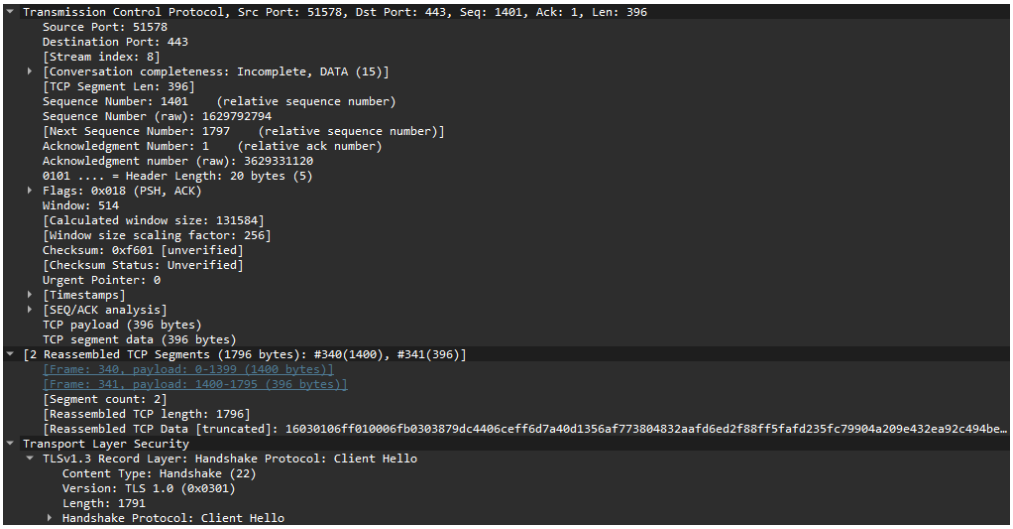
3. En el caso del protocolo TCP, la trama tiene esta información.



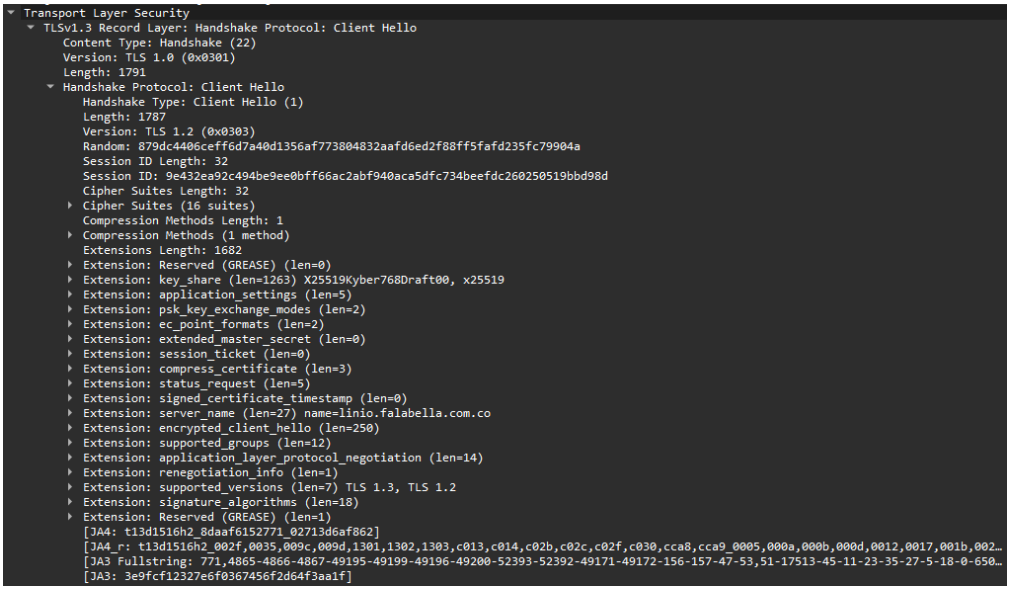
Nombre	Bits	Descripción	Valor
Source Port	16	Identifica el terminal de origen.	51578
Destination Port	16	Identifica el terminal de destino.	443
Sequence Number	32	Identifica el primer byte de datos.	0
ACK Number	32	Contiene el valor del próximo byte que está dispuesto a recibir.	0
Header Length	4	Longitud de cabecera para identificar el inicio de los datos.	32 bytes
Window	16	Cuantos bits componen la ventana de transmisión.	64240

Checksum	16	Se utiliza para detectar errores.	0xea46
Urgent Pointer	16	Sirve para indicar si los datos son urgentes.	0
TCP Options	32	Permite añadir campos a la cabecera.	

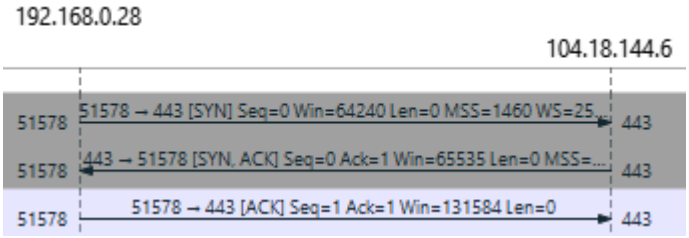
Las tramas que construidas usando el protocolo TLS contienen información de tamaño variable y están encapsulados en una capa adicional con información de seguridad.



En este caso, la capa de seguridad tiene 1791 bits de longitud y contiene información sobre el tipo, la id de sesión, valor aleatorio, etc.



4. En el siguiente diagrama se puede apreciar la comunicación entre el equipo local (192.168.0.1) y la página web del comercio (104.18.144.6) al realizar el saludo de tres vías.



Para realizar esta comunicación (en particular, la última de las tres), la trama TCP presenta un marcador ACK enviado desde el puerto 51578 del equipo cliente al puerto 443 del equipo servidor. Esta trama está encapsulada bajo el protocolo IPv4, con 128 saltos disponibles desde la dirección IP del cliente (192.168.0.28) a la del servidor (104.18.144.6). Finalmente, esta trama está contenida dentro del protocolo Ethernet II, con remitente, la interfaz del cliente (34-6F-24-A8-16-FB) y destinatario la interfaz del puerto de salida del enrutador (58-23-8C-57-77-51).

```
▾ Ethernet II, Src: AzureWaveTec_a8:16:fb (34:6f:24:a8:16:fb), Dst: VantivaUSA_57:77:51 (58:23:8c:57:77:51)
  ▸ Destination: VantivaUSA_57:77:51 (58:23:8c:57:77:51)
  ▸ Source: AzureWaveTec_a8:16:fb (34:6f:24:a8:16:fb)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 192.168.0.28, Dst: 104.18.144.6
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 40
    Identification: 0xed5e (60766)
  ▸ 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x5494 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.0.28
    Destination Address: 104.18.144.6
▸ Transmission Control Protocol, Src Port: 51578, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

5. Ruta seguida hasta el servidor DNS:

```
Traza a la dirección megacenter-1-cache-res.claro.net.co [190.157.8.109]
sobre un máximo de 30 saltos:

  1   103 ms     5 ms     3 ms  192.168.0.1
  2    16 ms    15 ms    37 ms  dynamic-ip-190841801.cable.net.co [190.84.180.1]
  3    29 ms    15 ms    28 ms  172.21.18.58
  4    17 ms    20 ms    23 ms  100.65.53.1
  5    14 ms    13 ms    19 ms  100.65.53.2
  6    16 ms    20 ms    16 ms  dynamic-ip-1868612665.cable.net.co [186.86.126.65]
  7    14 ms    15 ms    57 ms  megacenter-1-cache-res.claro.net.co [190.157.8.109]
```

Ruta seguida hasta la página de Linio:

```
Traza a 104.18.144.6 sobre caminos de 30 saltos como máximo.

  1     3 ms     2 ms     2 ms  192.168.0.1
  2    17 ms    15 ms    49 ms  dynamic-ip-190841801.cable.net.co [190.84.180.1]
  3    16 ms    13 ms    17 ms  172.21.18.58
  4     *        *      154 ms  comunicacin-ic-321792.ip.twelve99-cust.net [213.248.70.69]
  5   102 ms     *        *     mai-b2-link.ip.twelve99.net [213.248.70.68]
  6    72 ms    67 ms    88 ms  cloudflare-ic-363850.ip.twelve99-cust.net [62.115.167.113]
  7    60 ms    64 ms    77 ms  108.162.211.236
  8    62 ms    57 ms    61 ms  104.18.144.6
```

En este caso, las únicas direcciones IP conocidas en el trayecto son 192.168.0.1, interfaz de la puerta de salida en el enrutador de casa y las direcciones IP destino que corresponden al servicio de DNS de Telmex, Bogotá (192.157.8.109) y a Falabella, que aloja el sitio de Linio (192.18.144.6). Las demás IPs en el camino son desconocidas.

Preguntas:

- El puerto origen es 51578.
- No está reservado para ningún uso definido, es un puerto privado del cliente.
- El puerto destino es 443.
- El puerto 443 está reservado para https, es un puerto bien conocido en el servidor.
- El marcador establecido es 0x010 (ACK)
- El número de secuencia relativo es 1.

CONCLUSIONES

- El saludo de tres vías es muy importante al establecer una conexión confiable en redes TCP/IP. Este proceso asegura que tanto el cliente como el servidor están sincronizados y listos para intercambiar datos, lo que permite mantener la integridad de la comunicación en aplicaciones en aplicaciones web.
- Wireshark es una herramienta fundamental para el análisis del tráfico de red. Su capacidad para identificar y describir tramas de múltiples protocolos de comunicación permite realizar análisis detallados de la seguridad y eficiencia de la red.
- El protocolo Ethernet se ocupa de la comunicación inmediata. Aunque los contenidos de las capas de aplicación e internet no cambian, el protocolo Ethernet se actualiza con las direcciones MAC de cada máquina involucrada en un salto de red.
- La práctica de trazar rutas y entender la encapsulación de datos en diferentes niveles del modelo OSI permite identificar posibles cuellos de botella o vulnerabilidades en la red. Esto también permite una mejor comprensión de cómo los datos viajan desde el origen hasta el destino, facilitando el diagnóstico de problemas y la optimización del rendimiento de la red.