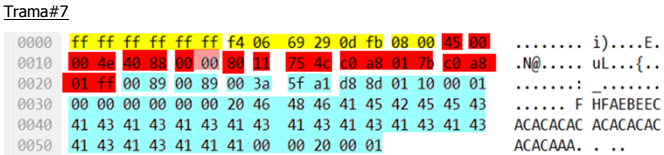
**2. PARA LAS TRAMAS ANTERIORES, SELECCIONE LAS OPCIONES CORRECTAS E INDIQUE LAS INCORRECTAS CON SUS FUNDAMENTOS:**



**Ethernet:**

**Mac Destino:** FF.FF.FF.FF.FF.FF

**Mac Fuente:** F4.06.69.29.0D.FB

**Protocolo:** IPv4 (0x800)

**IPv4:**

**Versión / Header Length:** 45 (0100|0101) → V: 4 ; HL: 5 (\*32 bits = 20 bytes)

**Tipo de Servicio**: 0

**Tamaño:** 004E (78 bytes)

**Identificación**: 40 88

**Flags:** 0 (0|0|0|0 0000) (Reservado|No fragmentado|Más fragmentos|5 bits Posición de Fragmento)

**Posición de Fragmento**: 0 0000 00000 00000 (13 bits en total: Primero 5 de Flags + 8)

**TTL**: 80 (128 saltos)

**Protocolo**: UDP (0x11)

**Header Checksum:** 754C

**IP Fuente**: C0 A8 01 7B (192.168.1.123)

**IP Destino**: C0 A8 01 FF (192.168.1.255)

**UDP**:

**Puerto Origen**: 0089 (137)

**Puerto Destino**: 0089 (137)

**Tamaño**: 003A (58 bytes)

**Checksum**: 5FA1

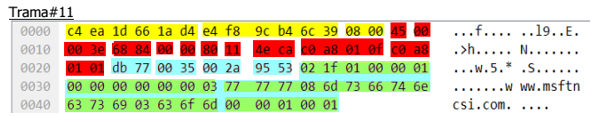
**Datos**: 50 bytes.

**a. La trama#7 es una trama Ethernet II que encapsula un datagrama IPv6.**

Falso. Encapsula un datagrama IPV4 (0x0800).

**b. La trama#7 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.20.**

Falso. Encapsula una trama IPV4 (0x0800) con UDP (0x11). La trama ARP es 0x0806.



**Ethernet:**

**Mac Destino**: c4.ea.1d.66.1a.d4

**Mac Fuente**: e4.f8.9c.b4.6c.39

**Protocolo**: IPV4 (0x800)

**Ipv4**:

**Versión / Header Length:** 45 (0100|0101) → V: 4 ; HL: 5 (20 bytes)

**Tipo de Servicio**: 0

**Tamaño:** 003E (62 bytes)

**Identificación**: 6884

**Flags:** 0 (0|0|**0**|0 0000).

**Posición de Fragmento**: 0 0000 00000 00000 (13 bits en total: Primero 5 de Flags + 8)

**TTL**: 80 (128 saltos)

**Protocolo**: UDP (0x11)

**Header Checksum:** 9553

**IP Fuente**: C0.A8.01.0F (192.168.1.15)

**IP Destino**: C0.A8.01.01 (192.168.1.1)

**UDP**:

**Puerto Origen**: DB77 (56183)

**Puerto Destino**: 0035 (53 , es el que utiliza DNS)

**Tamaño Mensaje**: 002A (42 bytes)

**Suma Verificación**: 9553

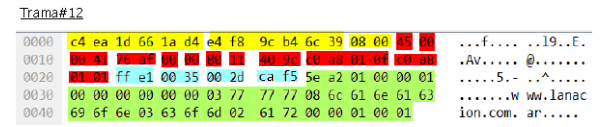
**Datos**: 34 bytes. [www.msftncsi.com](http://www.msftncsi.com) (desde 77 hasta 6d)

**c. La trama#11 posee una dirección MAC destino del tipo UNICAST, encapsula un datagrama IP sin fragmentar, originado en el host 192.168.1.15, que encapsula una solicitud DNS para el sitio www.msftncsi.com, sobre un segmento UDP con puerto origen 56183.**

Verdadero.

**d. La trama#11 corresponde a los 80 bytes de una trama Ethernet II, que encapsulan un datagrama IP sin fragmentar, enviado por el host 192.168.1.15 al servidor 192.168.1.1, para realizar una consulta DNS encapsulada sobre un segmento UDP.**

Falso. Son 76 bytes (Si considero el CRC 76+4 = 80 bytes, es Verdadero)



**Ethernet:**

**Mac Destino**: C4.EA.1D.66.1A.D4

**Mac Fuente**: E4.F8.9C.B4.6C.39

**Protocolo**: IPV4 (0x0800)

**IPv4**:

**Protocolo**: UDP (0x11)

**IP Fuente**: C0.A8.01.0F (192.168.1.15)

**IP Destino**: C0.A8.01.01 (192.168.1.1)

**UDP**:

**Puerto Origen**: FFE1 (65505)

**Puerto Destino**: 0035 (53)

**Tamaño Mensaje**: 002D (45 bytes)

**Checksum**: CAF5

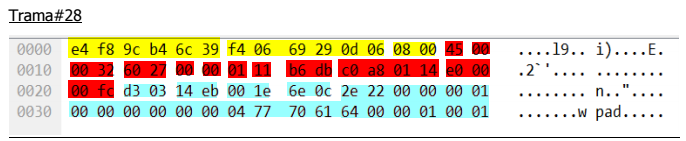
**Datos**: 37 bytes

**e. La trama#12 encapsula un mensaje unicast de MAC generado por un host de la red IP 192.168.1.0/24 con socket destino 192.168.1.1:53**

Verdadero.

**f. La trama#12 encapsula un broadcast de MAC generado por un host con MAC e4.f8.9c.b4.6c.39, correspondiente al host 192.168.1.15, con destino a la dirección IP 192.168.1.1, que encapsula un segmento TCP.**

Falso. Encapsula un segmento UDP (0x11)



**Ethernet:**

**Mac Destino:** E4 F8 9C B4 6C 39

**Mac Fuente:** F4 06 69 29 0D 06

**Protocolo**: IPv4 (0x0800)

**IPv4**:

**Protocolo**: UDP (0x11)

**IP Fuente**: C0 A8 01 14 (192.168.1.20)

**IP Destino**: E0 00 00 FC (224.0.0.252)

**UDP**:

**Puerto Fuente**: D303

**Puerto Destino**: 14EB

**Tamaño Mensaje**: 1E (30 bytes)

**Suma Verificación**: 6E0C

**Datos**: 22 bytes

**g. La trama#28 tiene MAC destino e4.f8.9c.b4.6c.39, MAC origen f4.06.69.29.0d.06 y encapsula un datagrama IP con host origen 192.168.1.20.**

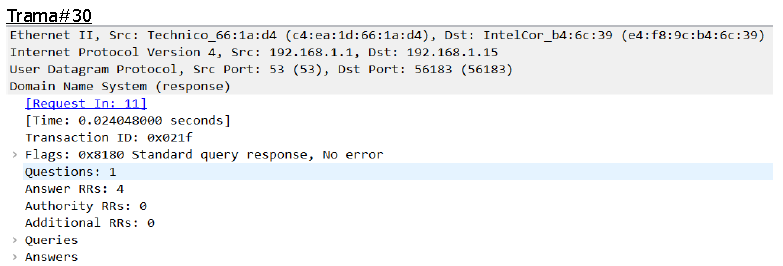
Verdadero.

**h. La trama#28 indica un broadcast de MAC y encapsula un datagrama IP con: dirección origen 192.168.1.20 e IP destino multicast, datos capa 3 correspondientes a un servicio sin conexión, no confiable, sin control de flujo, con detección de errores opcional (utilizado en este caso y que tiene un valor de 6e.0c).**

Falso. No indica un broadcast de MAC. Es Unicast E4 F8 9C B4 6C 39.

**i. La trama#28 es una trama unicast con IP origen 192.168.1.20. y es la respuesta a la trama#7.**

Falso. La IP de destino de la Trama#28 es distinta a la IP Fuente de la Trama#7 y la trama es multicast (Clase D).



**Ethernet**:

**Mac Fuente**: C4.EA.1D.66.1A.D4

**Mac Destino**: E4.F8.9C.B4.6C.39

**IPv4**:

**IP Fuente**: 192.168.1.1

**IP Destino**: 192.168.1.15

**DNS**:

**Puerto Fuente**: 53.

**Puerto Destino**: 56183.

**j. La trama#30 es la respuesta a la solicitud DNS de la trama#11**

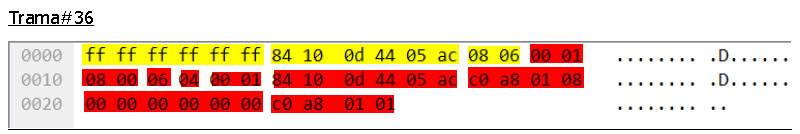
Verdadero. Standard Query Response. Request In: 11.

**k. La trama#30 indica que el nodo 192.168.1.15 ha enviado una consulta estándar DNS para el sitio www.msftncsi.com.**

Verdadero.

**l. La trama#30 señala que el host 192.168.1.1 brinda el servicio DNS al segmento IP respectivo y se identifica en la LAN con dirección MAC c4.ea.1d.66.1a.d4.**

Verdadero.



**Ethernet**:

**MAC Destino**: FF.FF.FF.FF (Broadcast).

**MAC Fuente**: 84.10.0D.44.05.AC

**Protocolo**: ARP (0x0806)

**ARP**:

**Tipo Hardware**: 1 (Ethernet)

**Tipo de Protocolo**: 0800 (IPv4)

**Tamaño Hardware**: 6

**Tamaño Protocolo**: 4

**Operación**: 1 (Request)

**Emisor MAC**: 84.10.0d.44.05.AC

**Emisor IP**: C0.A8.01.08 (192.168.1.8)

**Receptor MAC**: 00.00.00.00.00.00

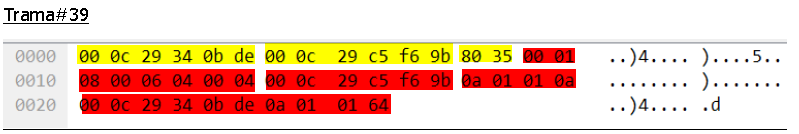
**Receptor IP**: C0.A8.01.01 (192.168.1.1)

**m. La trama#36 es una trama Ethernet II que encapsula un datagrama IP (0800).**

Falso. Encapsula ARP (0806)

**n. La trama#36 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.1.**

Verdadero.



**Ethernet**:

**MAC Destino**: 00.0C.29.34.0B.DE

**Mac Fuente**: 00.0C.29.C5.F6.9B

**Protocolo**: RARP (0x08035)

**RARP**:

**MAC Destino**: 00.0C.29.C5.F6.9B

(En rojo se marca solamente la MAC, el resto no sé bien cómo dividirlo)

**o. La trama#36 es una trama de solicitud de resolución de dirección MAC para la IP 192.168.1.1. y la respuesta es dada en la trama#39.**

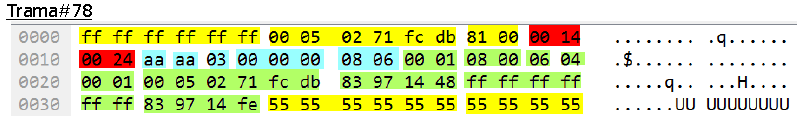
Falso. La trama 39 encapsula RARP (Reverse ARP) (0x8035) y no es la respuesta de ARP.

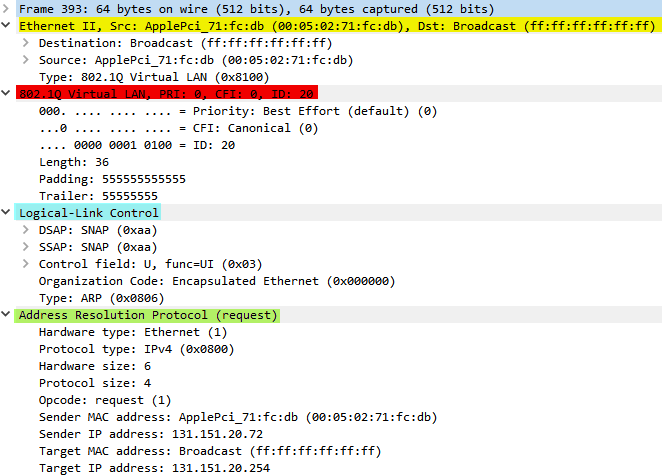
**p. La trama#39 tiene MAC destino 00.0c.29.34.0b.de, MAC origen 00.0c.29.c5.f6.9b y encapsula un datagrama IP (0800) con host destino 10.1.1.100.**

Falso. Encapsula un datagrama RARP.

**q. La trama#39 tiene MAC destino 00.0c.29.34.0b.de, MAC origen 00.0c.29.c5.f6.9b y encapsula un protocolo de resolución de dirección IP desconocida que le corresponda a la MAC origen.**

Verdadero. Eso realiza RARP, pregunta por la IP que le corresponde a su IP.



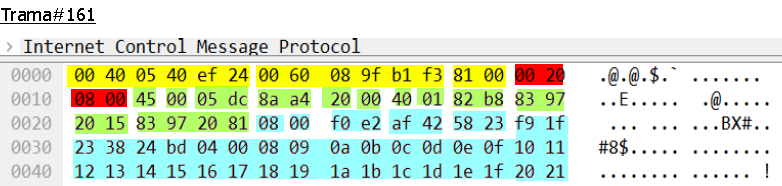


**r. La trama#78 posee una dirección MAC origen del tipo UNICAST, encapsula un datagrama IP sin fragmentar, originado en el host 131.151.20.72, que encapsula una solicitud DNS para el sitio www.google.com.ar, sobre un segmento UDP con puerto origen 56183.**

Falso. Es una trama VLAN que encapsula una solicitud ARP.

**s. La trama#78 indica que el nodo 131.151.20.72 ha enviado una solicitud ARP consultando la MAC que le corresponde al host IP 131.151.20.254.**

Verdadero**.**



**Ethernet:**

**MAC Destino:** 00.40.05.40.EF.24

**MAC Fuente:** 00.60.08.9F.B1.F3

**Protocolo:** VLAN(8100)

**VLAN**:

**Prioridad|CFI|ID:** 0020 (000|0|**0000 0010 0000**) → 32

**Protocolo:** IPV4 (0800)

**IPv4:**

**Versión / Header Length:** 45 (0100|0101) → V: 4 ; HL: 5 (20 bytes)

**Tipo de Servicio**: 00

**Tamaño:** 05DC (1500 bytes)

**Identificación**: 8AA4

**Flags:** 20 (0|0|1|0 0000) (Reservado|No fragmentado|**Más fragmentos = 1** |5 bits Posición de Fragmento)

**Posición de Fragmento**: 0 0000 00000 00000 (13 bits en total: Primero 5 de Flags + 8)

**TTL**: 40 (64 saltos)

**Protocolo:** ICMP (0x1)

**Header Checksum:** 82B8

**IP Fuente**: 83.97.20.15 (131.151.32.21)

**IP Destino**: 83.97.20.81 (131.151.32.129)

**ICMP**:

**Tipo**: 08 (Ping)

**Código**: 00

**Checksum:** F0E2

**Identificador:** AF42

**Número de secuencia:** 5823

**Datos**.

**t. La trama#161 es la respuesta a la solicitud DNS de la trama#78.**

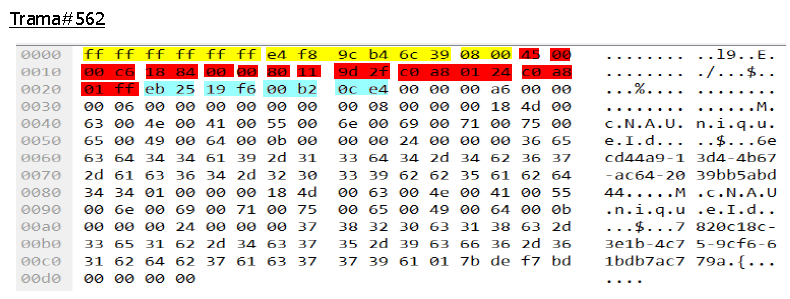
Falso. Es un solicitud Ping.

**u. La trama#161 Ethernet II corresponde a los 1.500 bytes de un datagrama IP fragmentado que proporciona direccionamiento a un paquete ICMP, enviado por el host 131.151.32.21 al host 131.151.32.129.**

Verdadero**.** Tiene campo tamaño de datagrama igual a 05DC (1500 bytes).

**v. La trama#161 señala que el host 131.151.32.21 pertenece a la VLAN 32, encapsula el primer paquete IP fragmentado con una solicitud de ECHO correspondiente al protocolo ICMP y se descartará luego de 64 saltos, en caso de no llegar a destino.**

Verdadero**.**



**Ethernet:**

**MAC Destino:** FF.FF.FF.FF.FF.FF → BROADCAST

**MAC Fuente:** E4.F8.9C.B4.6C.39

**Protocolo:** IPv4(0800)

**IPv4:**

**Versión / Header Length:** 45 (0100|0101) → V: 4 ; HL: 5 (20 bytes)

**Tipo de Servicio**: 00

**Tamaño:** 00C6 (198 bytes)

**Identificación**: 1884

**Flags:** 00 (0|0|0|0 0000)

**Posición de Fragmento**: 0 0000 00000 00000 (13 bits en total: Primero 5 de Flags + 8)

**TTL**: 80 (128 saltos)

**Protocolo:** UDP (0x11)

**Header Checksum:** 9D2F

**IP Fuente**: C0.A8.01.24 (192.168.1.36)

**IP Destino**: C0.A8.01.FF (192.168.1.255)

**UDP:**

**Puerto Fuente:** EB25 (60197)

**Puerto Destino:** 19F6 (6646)

**Tamaño:** 00B2 (178 bytes)

**Checksum:** 0CE4

**Datos**: 170 bytes.

**w. La trama#562 encapsula un broadcast de MAC generado por un host de la red 192.168.1.0/24 con IP destino a la dirección de broadcast de esa red.**

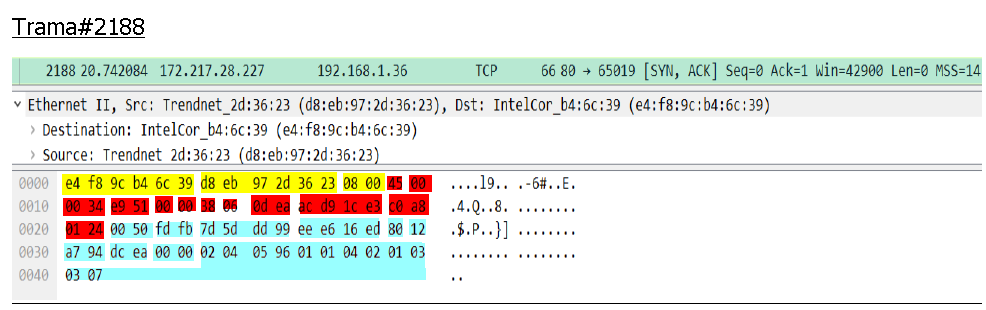
Verdadero. La ip 192.168.1.36 pertenece a la red 192.168.1.0/24.

**x. La trama#562 encapsula un broadcast de MAC generado por un host con MAC e4.f8.9c.b4.6c.39, perteneciente a la red 192.168.1.0/24, con destino a la dirección IP 192.168.1.1.**

Falso. La dirección IP de destino es 192.168.1.255.

**y. La trama#562 encapsula un broadcast de MAC generado por el host 192.168.1.36 con IP destino a la dirección 192.168.1.255, sin fragmentar, que encapsula un segmento UDP con 170 bytes de datos.**

**Verdadero.** El Tamaño del datagrama es 178 bytes (8 bytes de cabecera + 170 bytes de datos)



**Ethernet:**

**MAC Destino:** E4.F8.9C.B4.6C.39

**MAC Fuente:** D8.EB.97.2D.36.23

**Protocolo:** IPv4(0800)

**IPv4:**

**Versión / Header Length:** 45 (0100|0101) → V: 4 ; HL: 5 (20 bytes)

**Tipo de Servicio**: 00

**Tamaño:** 0034 (52 bytes)

**Identificación**: E951

**Flags:** 00 (0|0|0|0 0000)

**Posición de Fragmento**: 0 0000 00000 00000 (13 bits en total: Primero 5 de Flags + 8)

**TTL**: 38 (56 saltos)

**Protocolo:** TCP (0x06)

**Header Checksum:** 0DEA

**IP Fuente**: AC.D9.1C.E3 (172.217.28.227)

**IP Destino**: C0.A8.01.24 (192.168.1.36)

**TCP**:

**Puerto fuente:** 0050 (80)

**Puerto destino:** FDFB (65019)

**Número de Secuencia:** 7D5DDD99 (2103303577)

**Número de Ack:** EEE616ED (4008056557)

**Tamaño de Cabecera:** 80 (**1000** 0000) → 8\*4 = 32 bytes

**Flags**: 000|0|0|0|0|1|0|0|1|0 (8012: 1000 **0000 0001 0010**) → Ack = 1 | Syn = 1

(Res|NS|CWR|ECE|URG|ACK|PSH|RST|SYN|FIN)

**Tamaño de Ventana**: A794 (42900 bytes)

**Checksum**: DCEA

**Puntero Urgente:** 0000

**Opciones**: 0204**0596**0101040201030307 →

**Kind**: 0x02

**Length**: 0x04

**MMS**: 0x0596 = 1430 bytes

**Otros**.

**z. La trama#2188 indica que el servidor HTTP con IP 172.217.28.227 confirma la recepción de solicitud de conexión del host 192.168.1.36 y propone un valor de tamaño de ventana de 42.900 bytes y tamaño máximo de segmento de 1.430 bytes.**

Verdadero.

MSS es igual a la diferencia MTU - Cabecera TCP - Cabecera IP

**Para el caso de Tramas#(varias):**



**aa. Las tramas #2182, #2188 y #2190 encapsulan 3 segmentos, respectivamente, el establecimiento de conexión entre el host 192.168.1.36 y el servidor 172.217.28.227, que acuerdan un tamaño de ventana de 42.900 bytes.**

Verdadero**.**

Primer paquete (SYN): SeqC: 0 ;

Segundo paquete (SYN+ACK): SeqS = 0 ; AckS = SeqC + 1 = 1 ;

Tercer paquete (ACK): AckC = SeqS + 1 = 1 ; SeqC =+ 1 = 1

El tamaño de ventana lo acuerda el receptor en el segundo paquete: 42900 bytes.



**bb. La trama#2202 indica que el servidor HTTP con IP 172.217.28.227 confirma la recepción del segmento con número de secuencia SEQ=287 e identifica, con un valor de 2128, la posición de los datos del segmento en el flujo de datos del host 192.168.1.36.**

Falso.El que está confirmando recepción de un paquete es el host (192.168.1.36)



**cc. La trama#2202 es una confirmación del segmento TCP encapsulado en la trama#2201, siempre y cuando la trama #2201 tuviera un valor SEQ=1431 y el segmento TCP transmitiera 697 bytes de datos.**

Verdadero.

2201 → Seq = 1431 (El tamaño total de la trama es de 751 - 14 Ethernet - 20 IP - 20 TCP = 697 bytes de datos)

2202 → Ack = 1431 + 697 =2128

**3. RESUELVA LOS SIGUIENTES EJERCICIOS:**

**a. ¿Cuál es el número mínimo de Bytes con que debe ejecutarse la aplicación PING extendido para que se produzca una fragmentación de un datagrama IP sobre Ethernet, con 44 paquetes? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).**

1 Paquete con Cabecera ICMP → 20 bytes cabecera IP + 8 cabecera ICMP + 1472 de datos

42 Paquetes Fragmentados IPV4 → 20 bytes cabecera IP + 1480 de datos

1472 bytes + 1480 bytes \* 42 + 1 byte = 63.633

**a. ¿Cuál es el número mínimo de Bytes con que debe ejecutarse la aplicación PING extendido para que se produzca una fragmentación de un datagrama IP sobre Ethernet, con 35 paquetes? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).**

1 Paquete con Cabecera ICMP → 20 bytes cabecera IP + 8 cabecera ICMP + 1472 de datos

33 Paquetes Fragmentados IPV4 → 20 bytes cabecera IP + 1480 de datos

1472 bytes + 1480 bytes \* 33 + 1 byte = 50.313

**b. ¿Cuál es el número de paquetes IP que se generan en una red con una MTU de 1000B si la aplicación de red HTTP encapsula 125990B en el protocolo de capa 4? Demuestre la fundamentación de su estimación o cálculo (al reverso de la hoja).**

Siendo que TCP maneja la fragmentación, necesito la cabecera TCP en todos los paquetes.

131 Paquetes fragmentados por TCP →20B Cabecera IP + 20B Cabecera TCP + 960B de datos

1 Paquete fragmentado por TCP →20B Cabecera IP + 20B Cabecera TCP + 230B de datos

A esto se le deberían sumar:

3 Paquetes para conexión TCP

4 Paquetes para desconexión TCP

Siendo un total de 139 Paquetes (suponiendo que no hay retransmisiones, y que la Window TCP está al máximo de una).

**c. ¿Qué valores tendrá el campo FLAGS en el primero, penúltimo y último paquete en caso de fragmentación IP?**

**FLAGS PRIMER PAQUETE:** 0x01 (como byte vale 0x20 porque tiene los 5 bits de la posición del fragmento)

**FLAGS PENÚLTIMO PAQUETE:** 0x01 (como byte vale 0x20 porque tiene los 5 bits de la posición del fragmento)

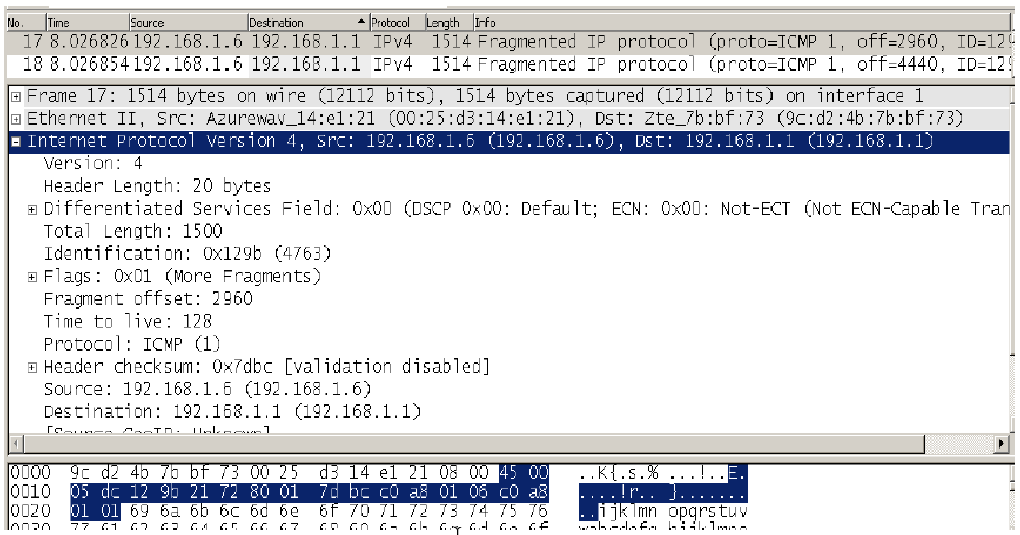
**FLAGS ÚLTIMO PAQUETE:** 0x00

bit 0: Reservado; debe ser 0

bit 1: 0 = Divisible, 1 = No Divisible (DF: Don’t Fragment)

bit 2: 0 = Último Fragmento, 1 = Fragmento Intermedio (le siguen más fragmentos) (MF: More fragments)

**d. En base a la captura responda:**



1. **¿Cómo se relacionan Header Length y Total Length?**Header Length está incluido en el Total Length.   
   En la captura, el total es 1500B y el Header 20B. Dejando 1480B para datos.
2. **¿En qué procesos intervienen los campos ID, FLAGS y FRAGMENT OFFSET, en el transmisor y receptor?**Se utilizan en la transmisión y recepción de tramas fragmentadas.  
   El ID me permite identificar de qué trama es un paquete que me llega.  
   El Offset me permite identificar el orden de los paquetes.  
   Los FLAGS me permiten identificar si el paquete es divisible o no, y si es el último fragmento de la trama.
3. **¿Para qué sirve el campo TTL con valor 128?**  
   El campo TTL especifica el número máximo de saltos por los que puede pasar un datagrama.  
   En este caso le permite 128 saltos antes de ser descartado.