2.5 Análisis de paquetes

En la Figura 7, puede observarse la información de los paquetes capturados durante el envío del nodo origen al nodo destino.
En la primera columna tenemos el número de frames capturados, en el frame número 1 se hace la negociación de la conexión entre el cliente y el servidor, en el cual el cliente manda una petición o solicitud de conexión, en el frame número 2 es donde el servidor ya acepta la conexión con el cliente, en el frame número 3 el cliente manda un mensaje al servidor que la conexión ha sido aceptada y a partir del frame número 4 el servidor empieza a enviar los paquetes de datos al cliente hasta llegar a su fin.
En la Segunda columna (time) se puede observar el tiempo que duró la transmisión, en la primera fila está en ceros puesto que no está enviando ningún paquete solo está en la negociación de la conexión, a partir de la segunda fila ya empieza el conteo del tiempo puesto que el servidor manda un mensaje al cliente diciendo que su conexión ha sido aceptada.
La tercera columna (source) nos indica las direcciones IP en el cual nos dice quien ha sido el que envía una petición o mensaje.
La cuarta columna (destination) corresponde a la dirección de a quién va dirigido la petición. La quinta columna (protocol) nos revela el tipo de protocolo de transporte que estamos utilizando para el tráfico de paquetes, en este caso estamos utilizando el Protocolo de Control de Transmisión (TCP) del modelo TCP/IP.
En la sexta columna (length) nos muestra el tamaño de envío en Bytes. En la séptima y última columna (info) se aprecia más información sobre el paquete.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.2	192.168.1.1	TCP	74	40736 > afs3-filese
2	0.000064010	192.168.1.1	192.168.1.2	TCP	74	afs3-fileserver > 4
3	0.001235701	192.168.1.2	192.168.1.1	TCP	66	40736 > afs3-filese
4	0.001619943	192.168.1.1	192.168.1.2	TCP	1091	[TCP segment of a r
5	0.001800849	192.168.1.1	192.168.1.2	TCP	1514	[TCP segment of a r
6	0.001917685	192.168.1.1	192.168.1.2	TCP	326	[TCP segment of a r
7	0.003082546	192.168.1.2	192.168.1.1	TCP	66	40736 > afs3-filese
8	0.003118283	192.168.1.2	192.168.1.1	TCP	66	40736 > afs3-filese
9	0.003140016	192.168.1.2	192.168.1.1	TCP	66	40736 > afs3-filese
10	0.003156840	192.168.1.1	192.168.1.2	TCP	66	afs3-fileserver > 4

Figura 7

En la Figura 8 se muestra el cómo se establece la conexión sucede a nivel de red entre el cliente y el servidor. En la negociación de tres vías el cliente con la dirección 192.168.1.2 le envía un segmento de sincronización (SYN) que contiene un identificador numérico al servidor (192.168.1.1). Al recibir esta información, el servidor tiene constancia de la intención de iniciar una comunicación por parte del cliente, además, gracias al identificador numérico recibido, conoce el punto exacto en el que el cliente señala el inicio de su transmisión de datos.

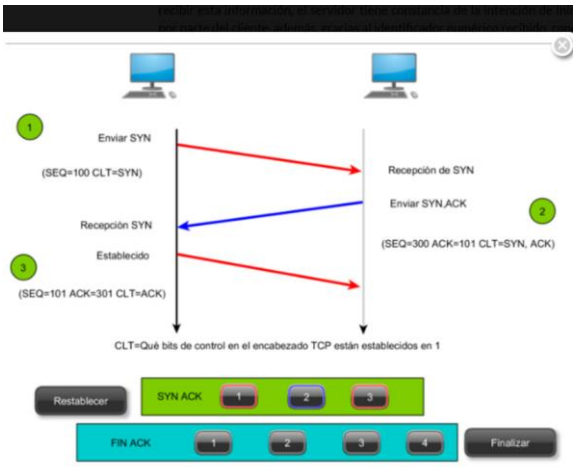

Figura 8

En la Figura 9 se muestra como termina una conexión TCP mediante cuatro vias. El servidor con la dirección de 192.168.1.1 envía un segmento FIN (no hay mas datos del emisor) al cliente 192.168.1.2, al recibir dicha información el cliente envía la respuesta de reconocimiento ACK al cliente. En la otra vuelta, ahora el cliente es quien envía dicho segmento FIN (no hay mas datos del emisor) al servidor y en la última vía el servidor es la que envía la respuesta ACK al cliente y con eso concluye la finalización de la negociación.

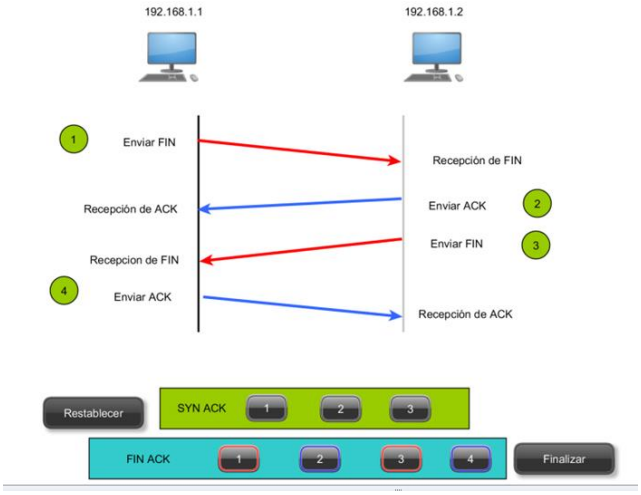

Figura 9

Cada vez que seleccionemos un frame, en la parte inferior nos mostrara información de lo que sucede en cada posición de acuerdo al protocolo TCP.
En la Figura 10, nos desglosa la información del frame seleccionado, en este caso en frame número 4 es aquél que se encuentra en la tercera columna de envío, cuyos campos se describen en seguida:
WTAP_ENCAP: 1 Se refiere al tipo de encapsulamiento, el 1 se refiere al Ethernet.
ARRIVAL TIME: nos muestra la fecha y tiempo de la captura.
FRAME LENGTH: nos muestra el tamaño de Bytes y a su lado el tamaño en bits, así mismo en la parte de abajo en Capture Length.

FRAME IS MARKED: nos manda un valor booleano (False), el cual significa que el usuario no ha marcado el marco, ósea trama.
FRAME IS IGNORED: de igual manera nos manda un booleano en el cual nos indica los paquetes han sido ignorados por lo tanto no han sido almacenados en el archivo de captura.
PROTOCOLS IN FRAME: De arriba hacia abajo, se indican las capas del **modelo TCP:** Acceso a la red, Internet y Transporte. Observando que en este mismo orden se encuentran las direcciones MAC, las direcciones IP y el número de puerto, tanto para el host origen como para el host destino.

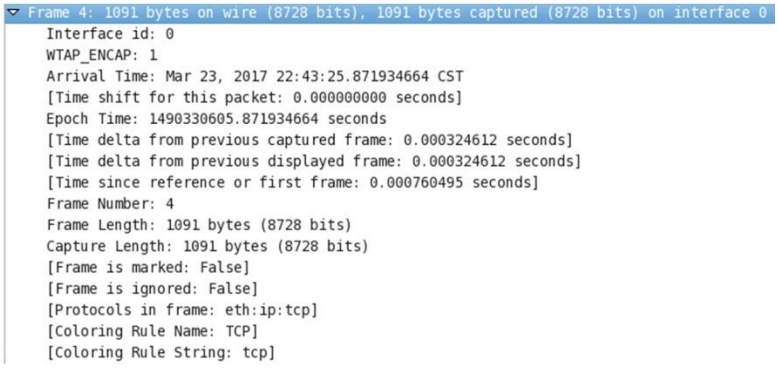

Figura 10

En la Figura 11, nos brinda información como el Origen (Src) donde nos muestra la dirección MAC, y nos indica el Destino (Dst) con su dirección MAC. (Una dirección MAC no puede ser repetida en este caso se está trabajando con una máquina virtual clonada por lo que conlleva a que tenga la misma dirección MAC.), desglosamos la información que contiene, el campo Destination nos muestra la dirección MAC del servidor así mismo en la parte de abajo muestra otra dirección (address) que es la del cliente, como lo acabamos de mencionar no puede haber una dirección MAC igual puesto que esto conllevaría a conflictos en los envíos de paquetes si hubiese sido de manera física la dirección MAC cambiaria. Así mismo nos muestra la dirección MAC del Origen (Source), como podemos observar en la Figura 21 nos muestra 4 bits desactivados 0, cuya dirección es UNICAST el cual es el envío de información desde un único emisor a un único receptor.

Figura 11

En la Figura 12, nos muestra las direcciones IP origen y la dirección IP destino.
VERSIÓN: Indica la versión del protocolo, en este caso se trata de IPv4.
HEADER LENGTH: Indica el tamaño de la cabecera.
TOTAL LENGTH: Muestra el tamaño total.
REVCERVED BIT: “Not set” significa que no se han reservado los bits.
DON’T FRAGMENT: “Set” indica que está activado y que no se fragmentó el conjunto de datos.

MORE FRAGMENTS: “Not set” significa que no hay más fragmentos, por lo tanto no está activado.
TIME TO LIVE (TTL): esto indica el tiempo de vida de cada paquete, en este caso su tiempo de vida fue de 64, su tiempo de vida no se mide con tiempo sino por **saltos**, lo que quiere decir que por cada router que pasa su tiempo de vida va disminuyendo, en caso que su tiempo de vida se acabe y no llegue a su destino esto el paquete se pierde totalmente.
PROTOCOL: TCP Nos indica el tipo de protocolo que se está utilizando
HEADER CHECKSUM: Si el envío concluyó correctamente este campo será igual a True, en otro caso False.

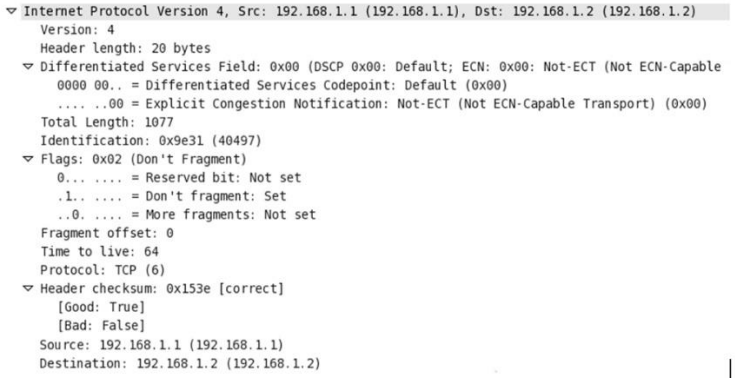

Figura 12

En la Figura 13 nos proporciona información acerca del número del puerto en este caso estamos utilizando el puerto 7000 para el Origen de envío, y el puerto 36638 para el destino, cuyos campos quedan descritos a continuación.
SOURCE PORT: afs3-fileserver (7000) nos está indicando que el servidor tiene el puerto 7000.
DESTINATION PORT: 36638 (36638) nos indica el puerto del cliente por el cual tendremos comunicación para hacer la transferencia de datos, ósea, en que puerto pasaran los datos.
HEADER LENGTH: 32 bytes, esta parte nos indica el tamaño de la cabecera de datos.
PUSH: “set” nos está indicando que el conjunto de empuje se activó.
WINDOWS SIZE VALUE: 227 es el valor del tamaño de la ventana.
CALCULATED WINDOW SIZE: 14528 Calcula el tamaño de la ventana.
CHECKSUM: 0x877b es el código de verificación para el control de errores.
TIMESTAMP: Marca de tiempo, tipo, tamaño, valor de la marca de tiempo.
NO. OPERATION: Operaciones como lo son copia en el fragmento, control de clases, numero de la operación.
TCP SEGMENT DATA: Nos está indicando el tamaño del segmento enviado, que en este caso es de 256.

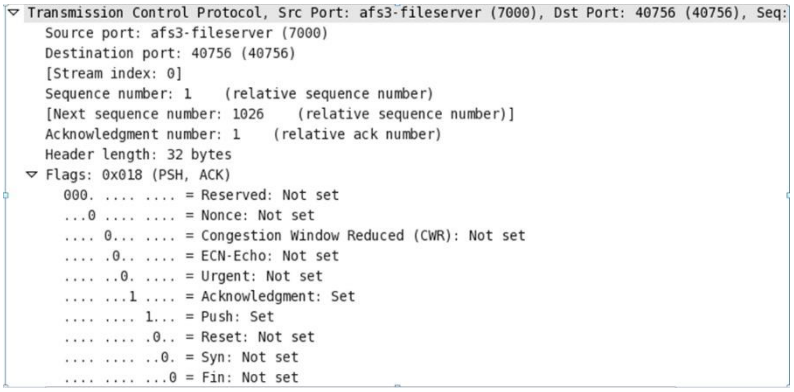

Figura 13