INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE CÓMPUTO

Redes de Computadoras

Práctica: WireShark

Prof.: Ricardo Martínez Rosales

Grupo: 2CM10

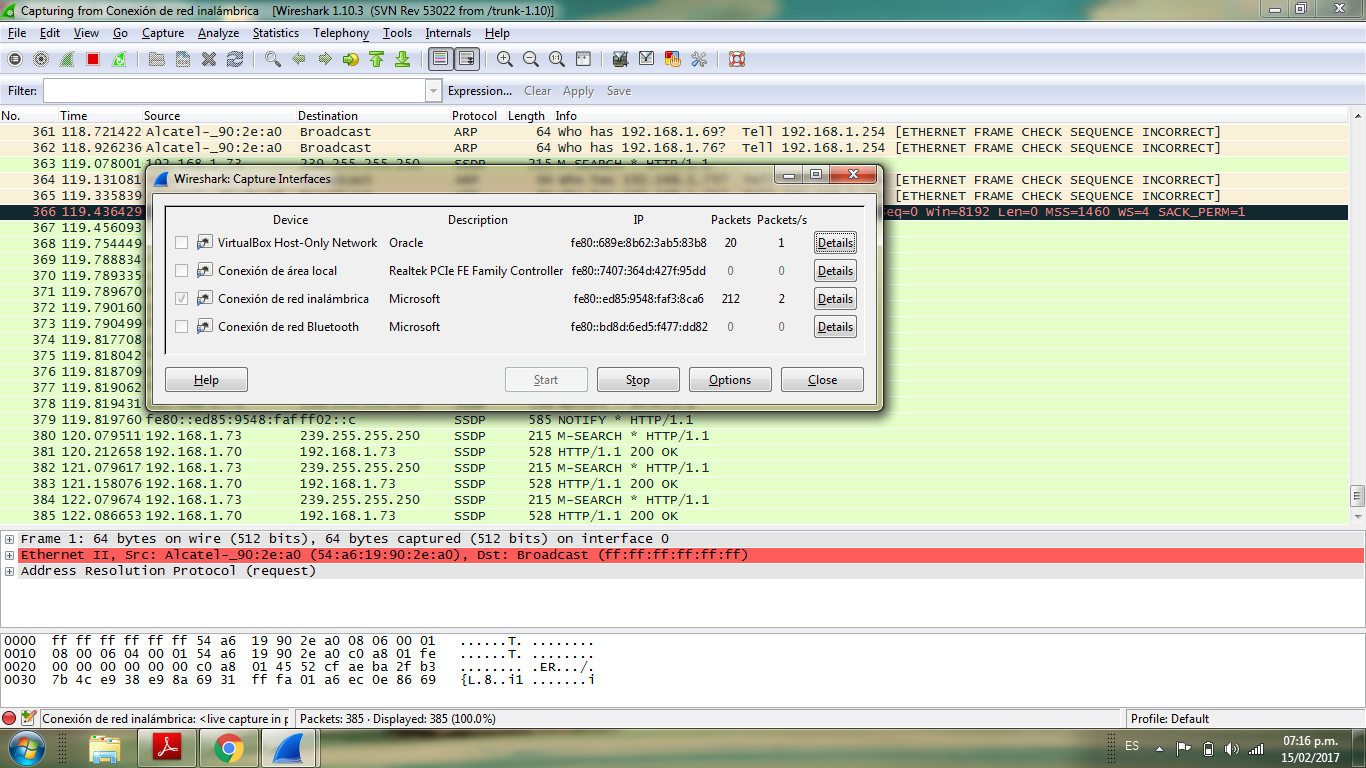
Alumno: Mendoza Parra Sergio.

Boleta: 2015630300

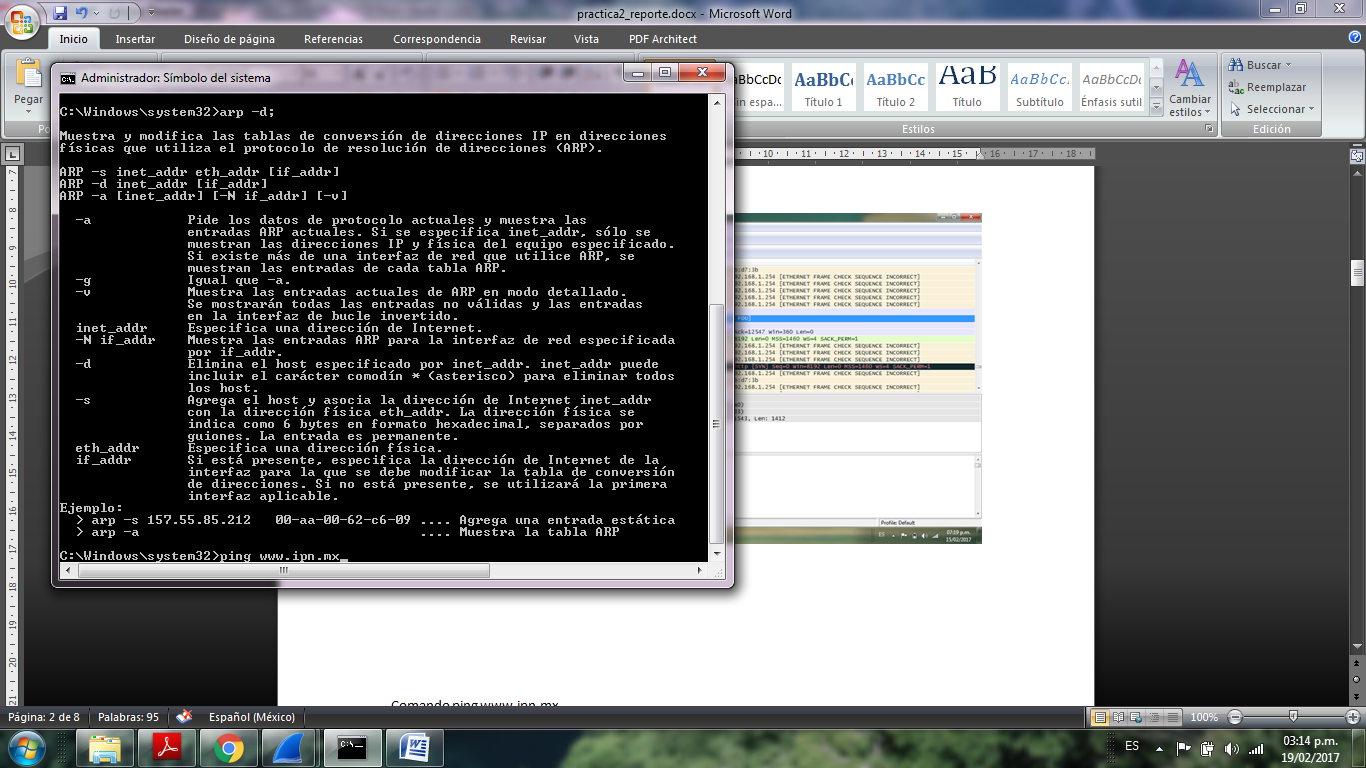
MEXICO, D.F. a 17 de Febrero del 2017

**Desarrollo de la práctica:**

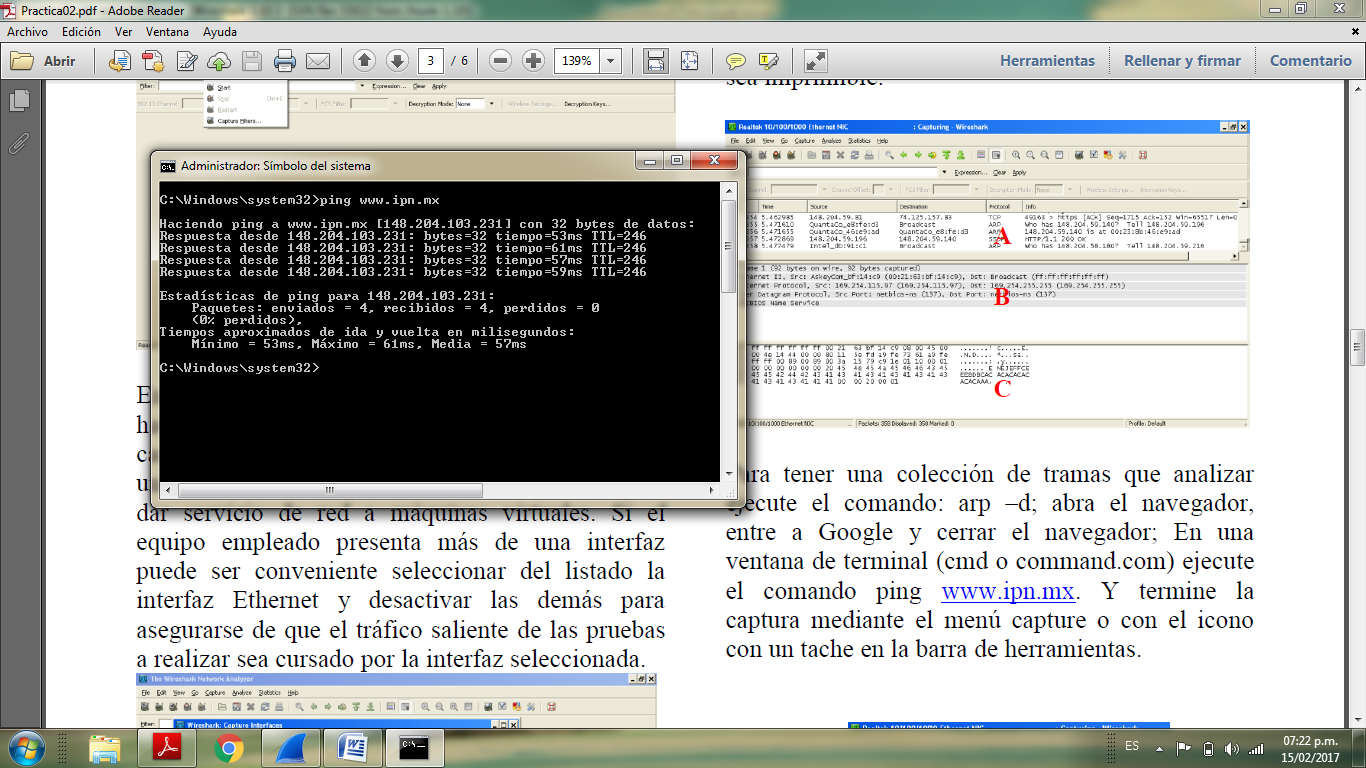
1.- Seleccioné el dispositivo de conexión de red inalámbrica y los demás los deshabilite.



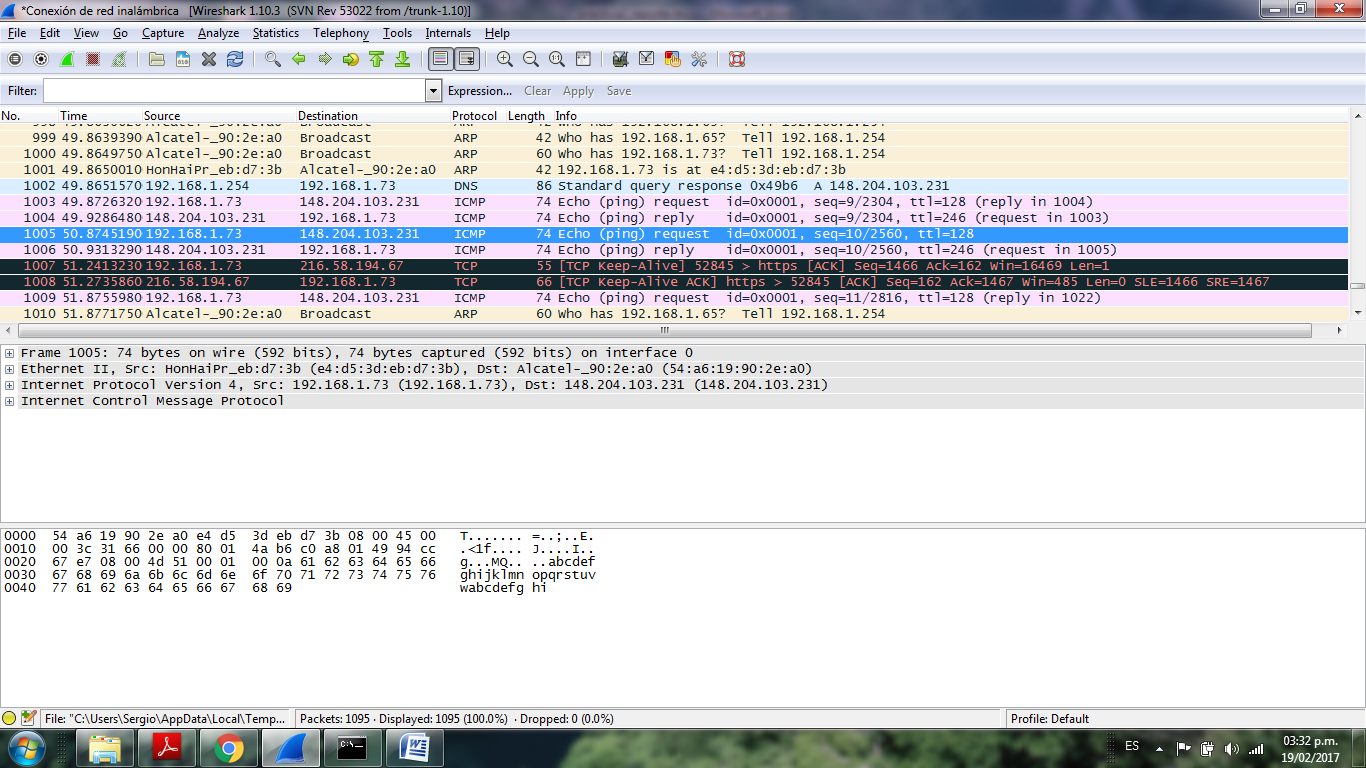
Después en el comando CMD ingresé el comando “arp –d;”, este comando elimina el host especificado por “inet\_addr. Inet\_addr”.



Después ingresé el comando “ping” seguido de la página “ [www.ipn.mx](http://www.ipn.mx) “como se muestra en la figura.



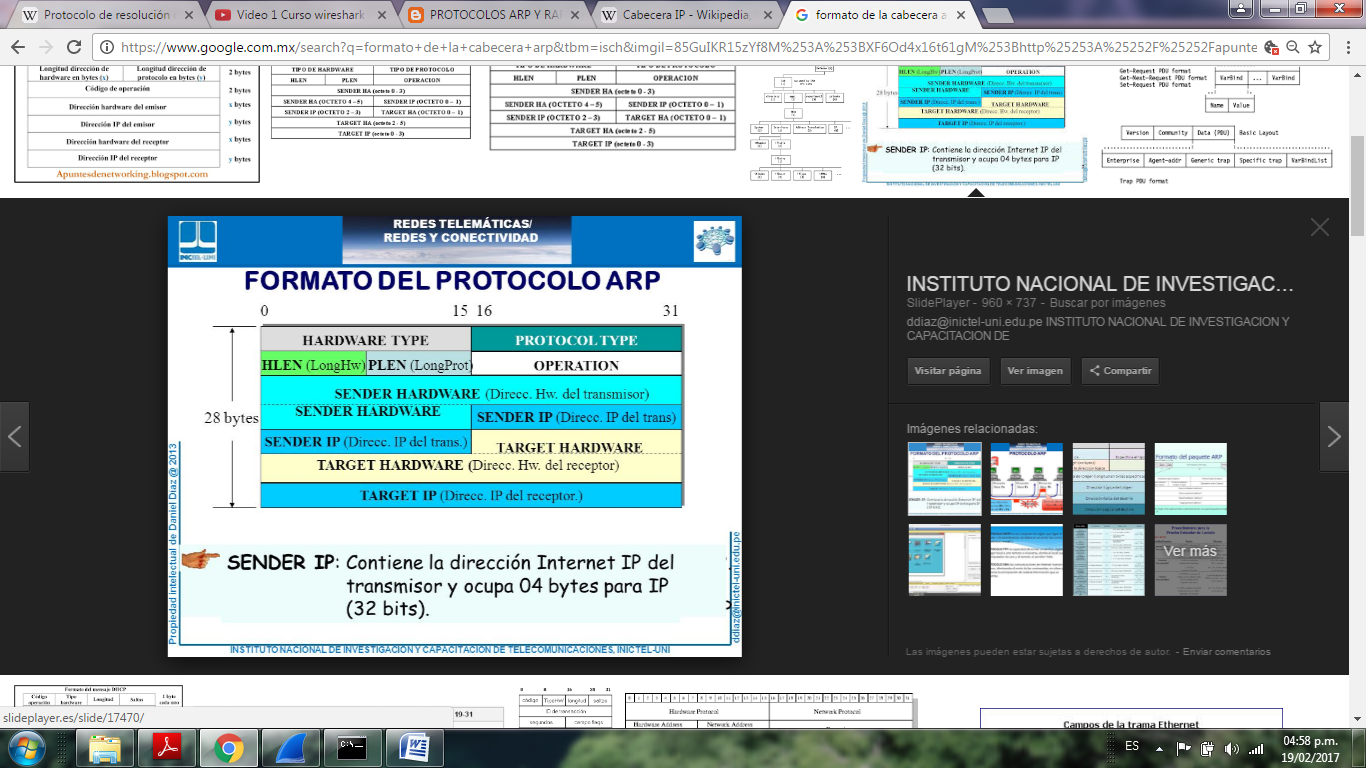
Una vez parando las capturas, estos fueron los protocolos que se vieron:



* **INVESTIGUE EL OBJETIVO Y FORMATO DE LA CABECERAS DE LOS PROTOCOLOS ENCONTRADOS**

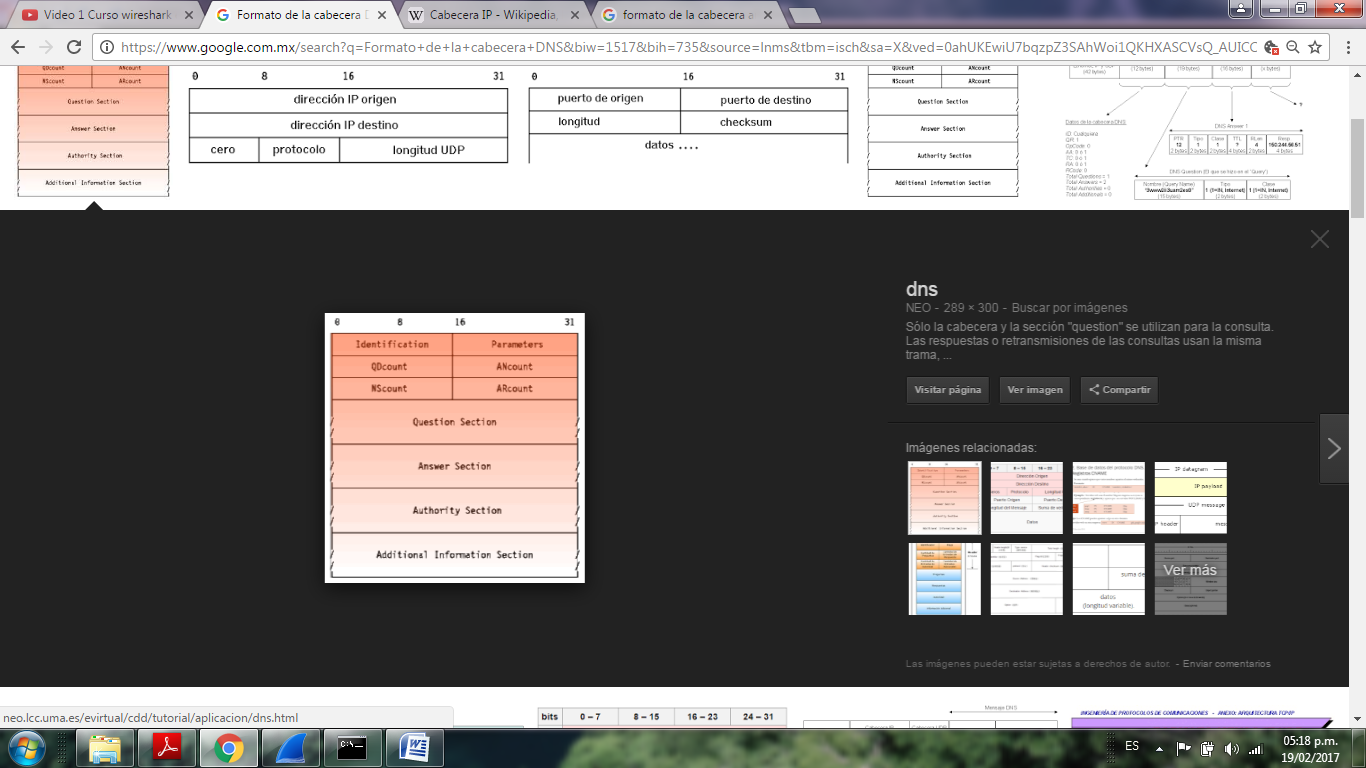
Protocolos encontrados en la captura:

* ARP (*protocolo de resolución de direcciones*): Es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete a la dirección de difusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina responda con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y las carga ARP permite a la dirección de Internet ser independiente de la dirección Ethernet pero esto solo funciona si todas las maquinas lo soportan.

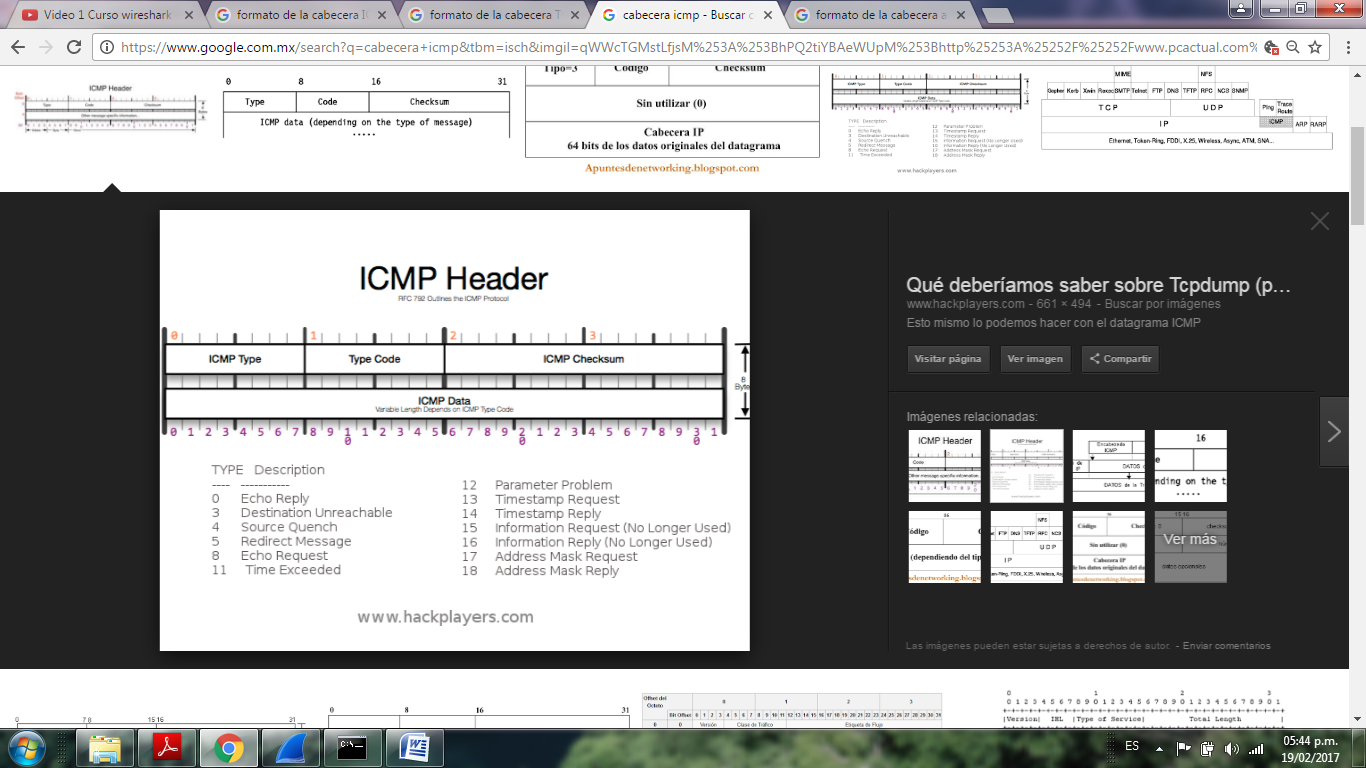


* DNS (*sistema de nombres de dominio*): Este protocolo se utiliza para recordad de manera sencilla las direcciones IP. De esta manera surge el concepto de nombres de dominio. Gracias a esto podemos asignar a una dirección IP un nombre, además de que es más fiables porque la dirección IP de un servidor puede cambiar pero el nombre no lo hace. Podemos decir entonces que el DNS es un sistema jerárquico y distribuido que permite traducir el nombre de dominio en direcciones IP y viceversa.

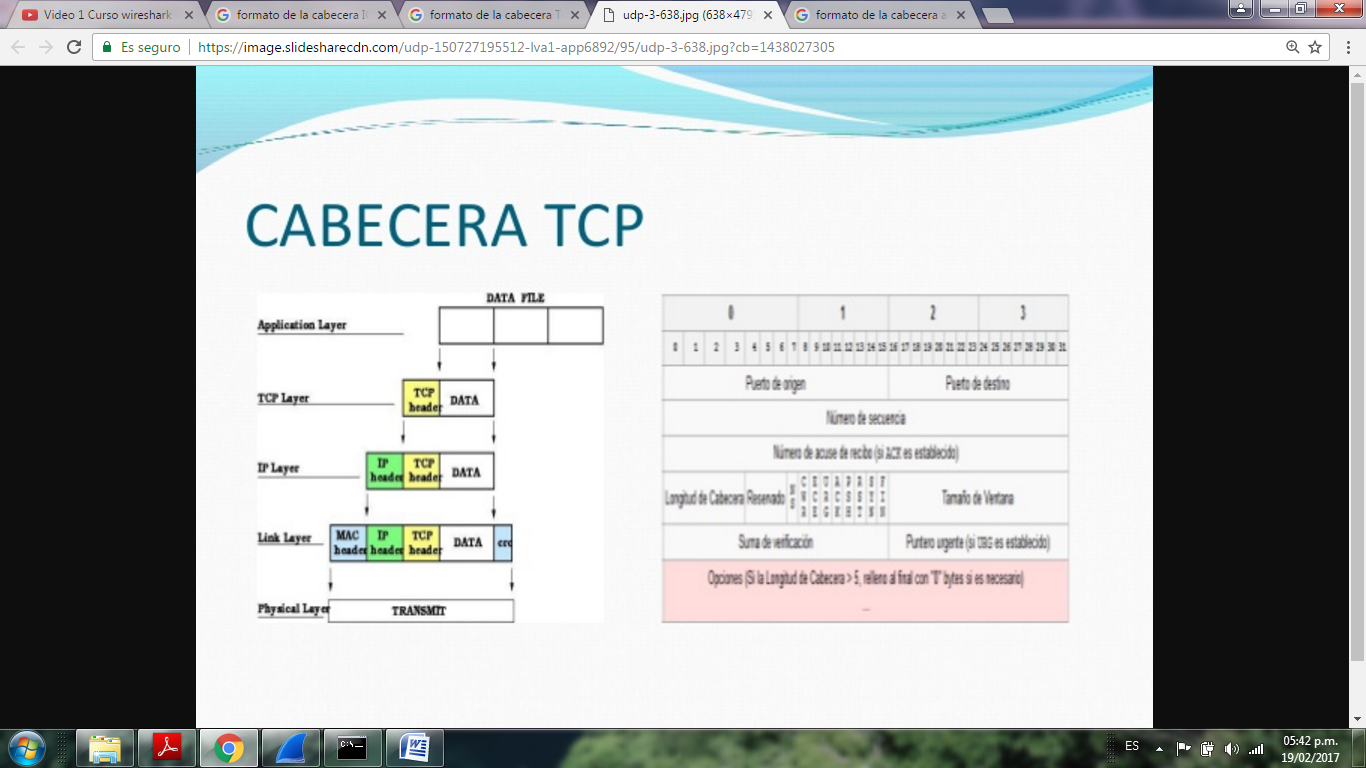
**FORMATO DE LA CEBECERA DNS**



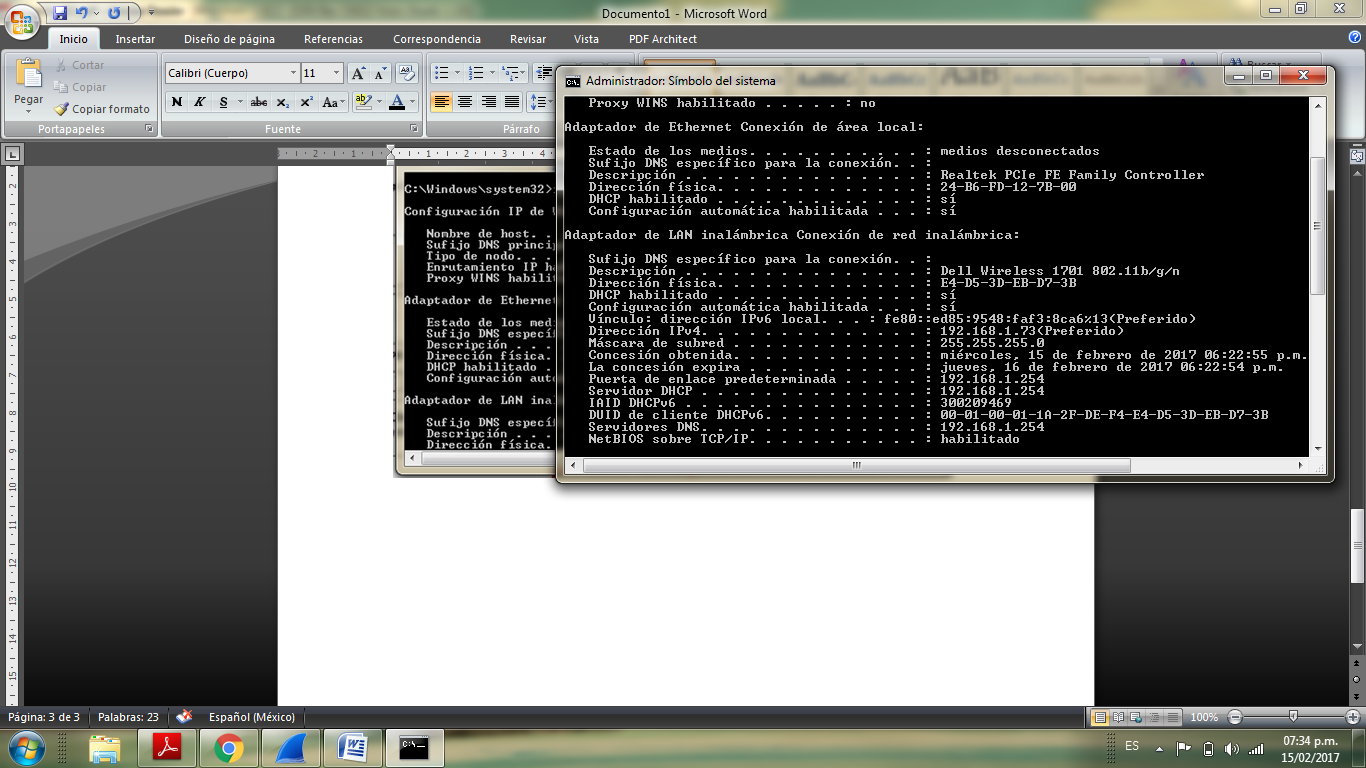
* ICMP (*Protocolo de mensajes de control de Internet*): Es un protocolo que permite administrar información relacionada con errores de los equipos en red. Si se tienen en cuenta los escasos controles que lleva a cabo el protocolo IP, ICMP no permite corregir los errores sino que los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es usado por todos los routers para indicar un error (llamado un *problema de entrega*).



* TCP (*Protocolo de Control de Transmisión*): Es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. En el nivel de aplicación, posibilita la administración de datos que vienen del nivel más bajo del modelo, o van hacia él, (es decir, el protocolo IP). Cuando se proporcionan los datos al protocolo IP, los agrupa en datagramas IP, fijando el campo del protocolo en 6 (para que sepa con anticipación que el protocolo es TCP). TCP es un protocolo orientado a conexión, es decir, que permite que dos máquinas que están comunicadas controlen el estado de la transmisión.



Después en el CMD se pone el comando “ipconfig/all” (ver imagen), el cual nos dice la dirección MAC que tiene nuestra computadora al igual que la dirección IP.

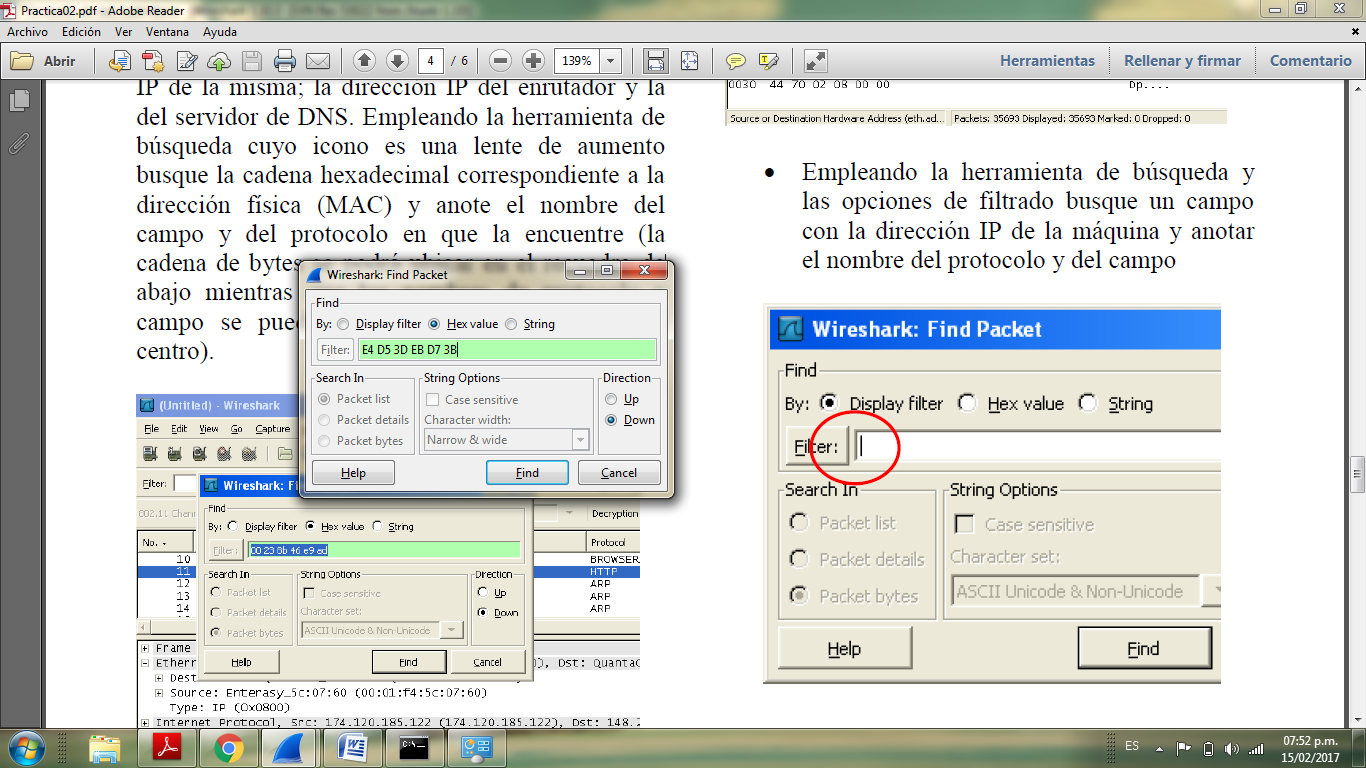


También nos dice la dirección IP del Router que nos sirve para interconectar redes de ordenadores e implementar puertas de acceso a internet y por último el servidor DNS que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder.

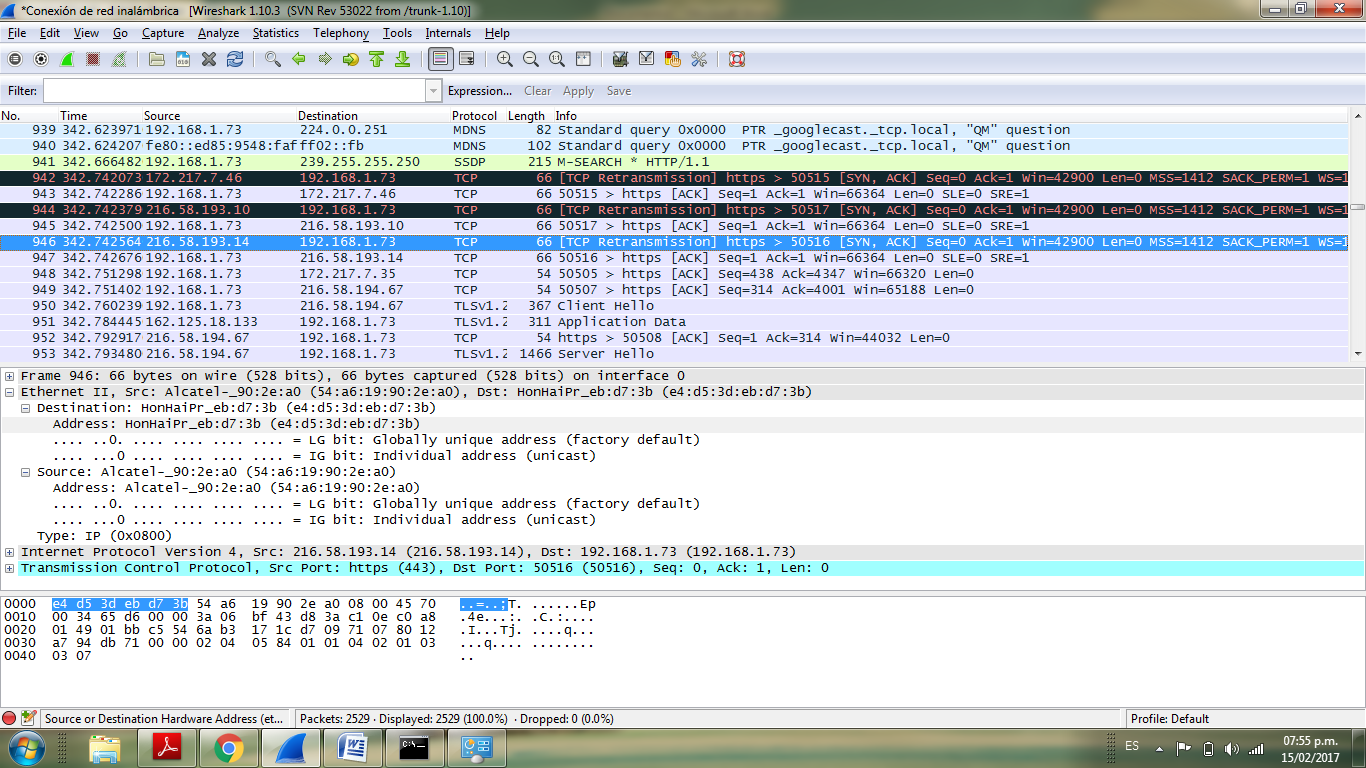
* **ANOTAR DIRECCION FISICA DE LA MAQUINA, ENRUTADOR, IP Y SERVIDOR DNS:**

|  |  |
| --- | --- |
| Dirección MAC: | E4-D5-3D-EB-D7-3B |
| Dirección IP: | 192.168.1.73 |
| Dirección IP Router: | 192.168.1.254 |
| Dirección del DNS: | 192.168.1.254 |

* **Empleando la herramienta de búsqueda cuyo icono es una lente de aumento busque la cadena hexadecimal correspondiente a la dirección física (MAC) y anote el nombre del campo y del protocolo en que la encuentre**



Después de ingresar la dirección MAC aparece seleccionado el campo, el protocolo y en la parte de abajo en la cadena de bytes, aparece de nuevo la dirección MAC que buscamos.

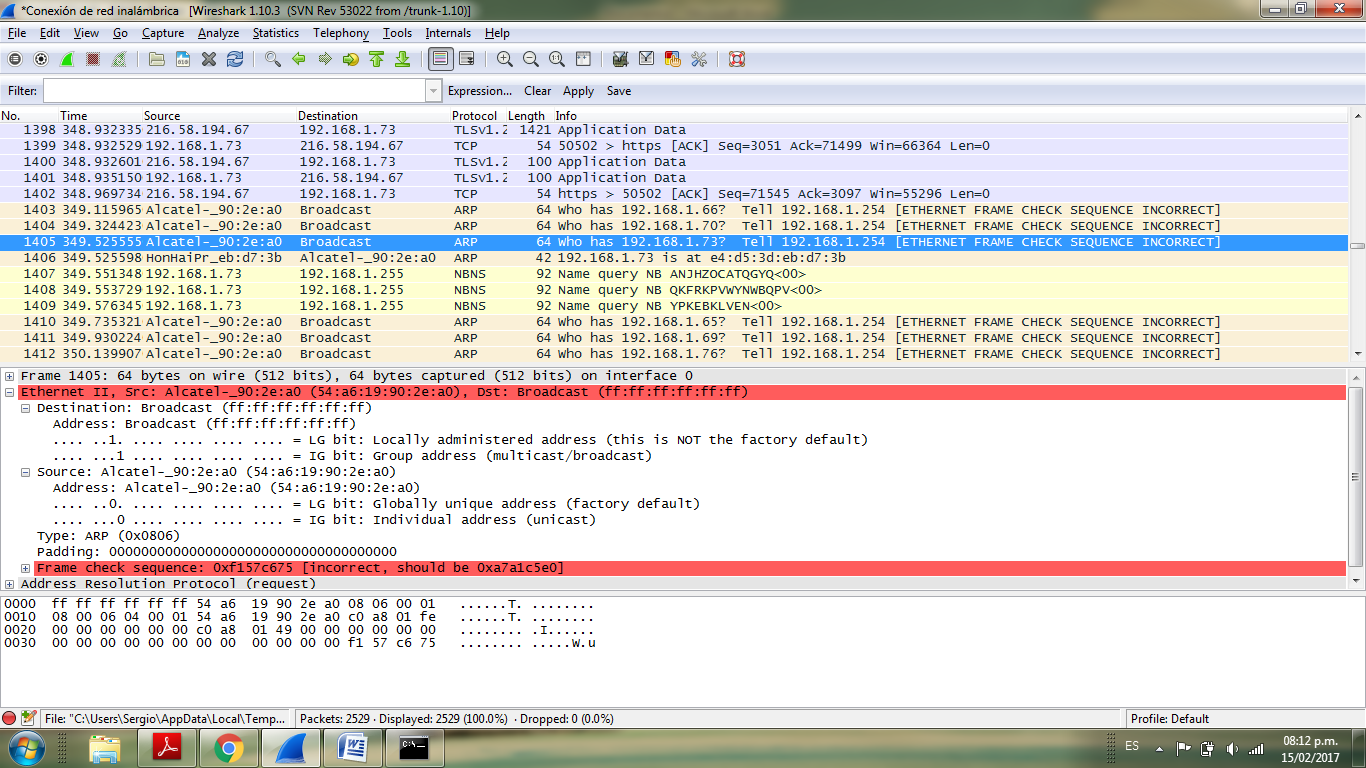


La dirección MAC se encuentra en:

* Protocolo: TCP
* **Empleando la herramienta de búsqueda y las opciones de filtrado busque un campo con la dirección IP de la máquina y anotar el nombre del protocolo y del campo:**

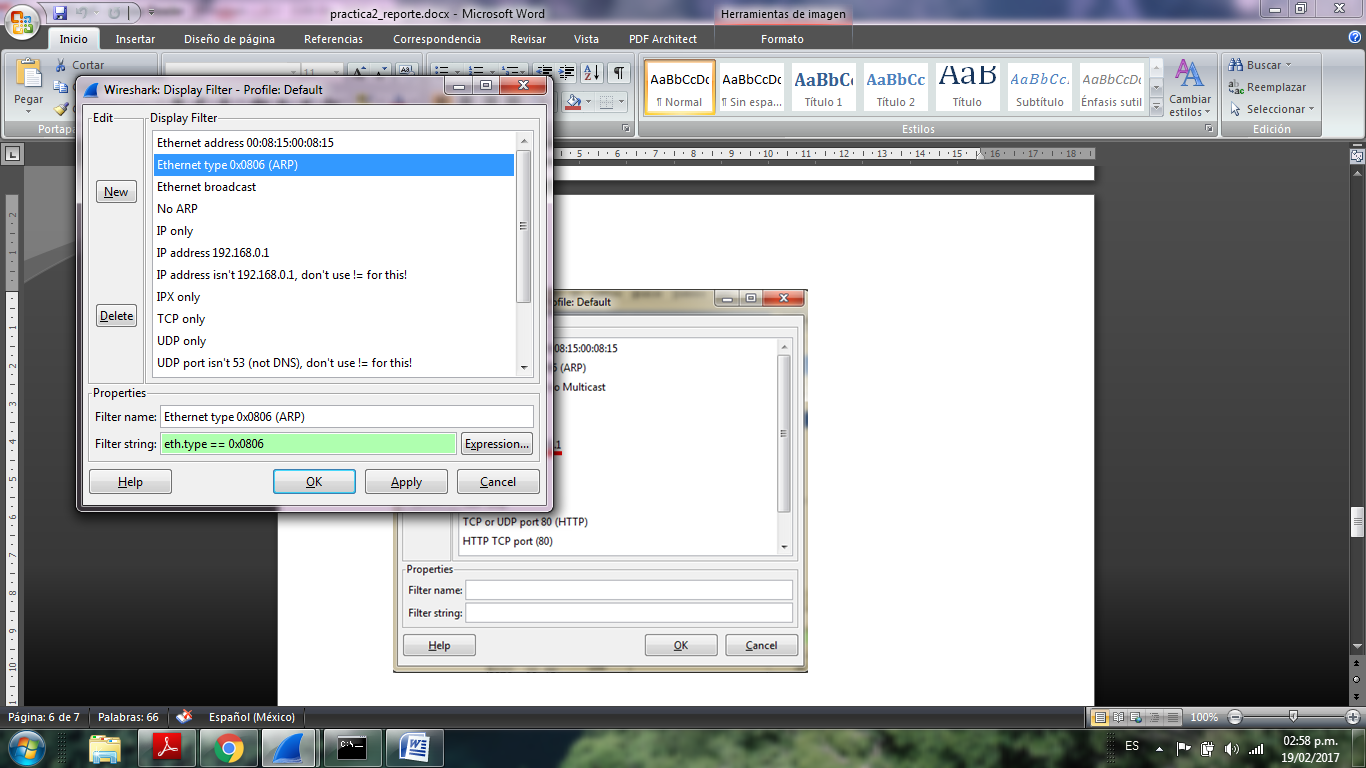


Lo encontrado de la dirección IP de la máquina:

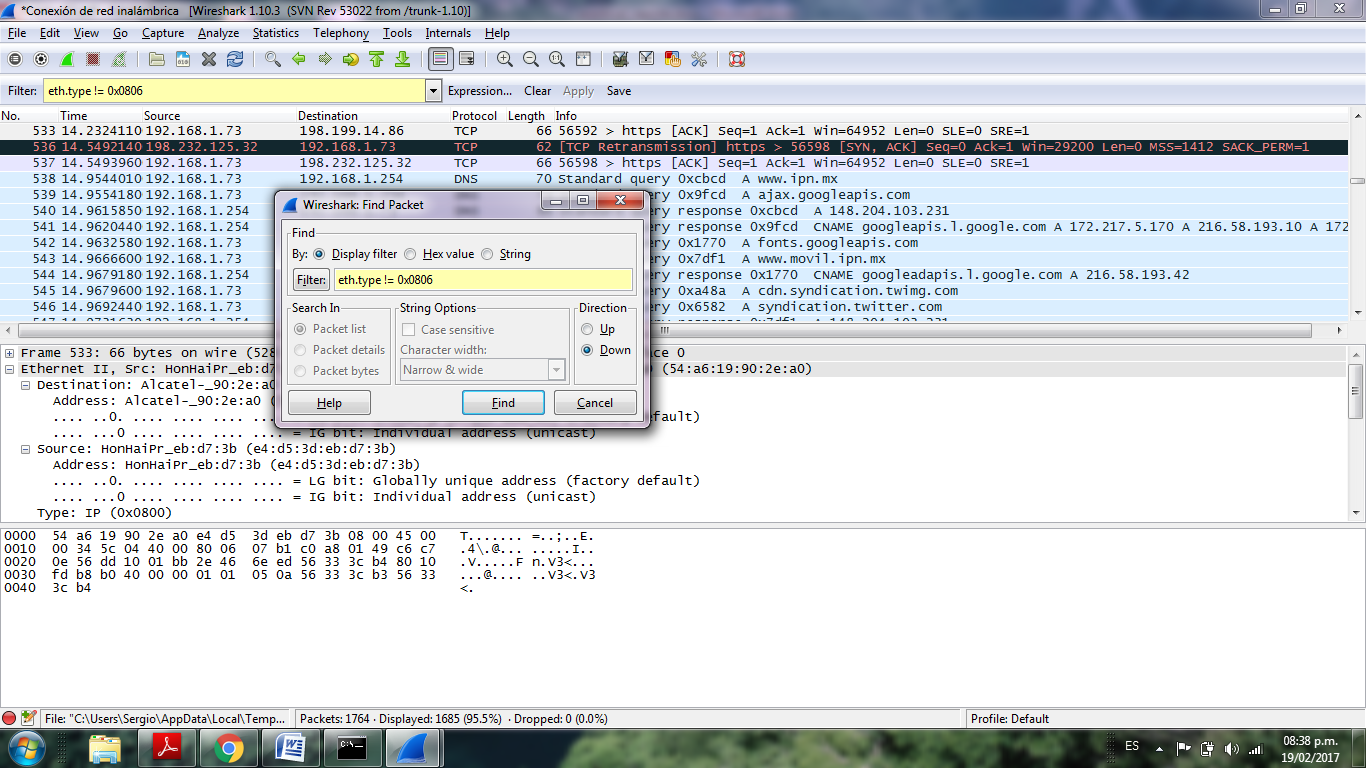


La dirección IP se encuentra en:

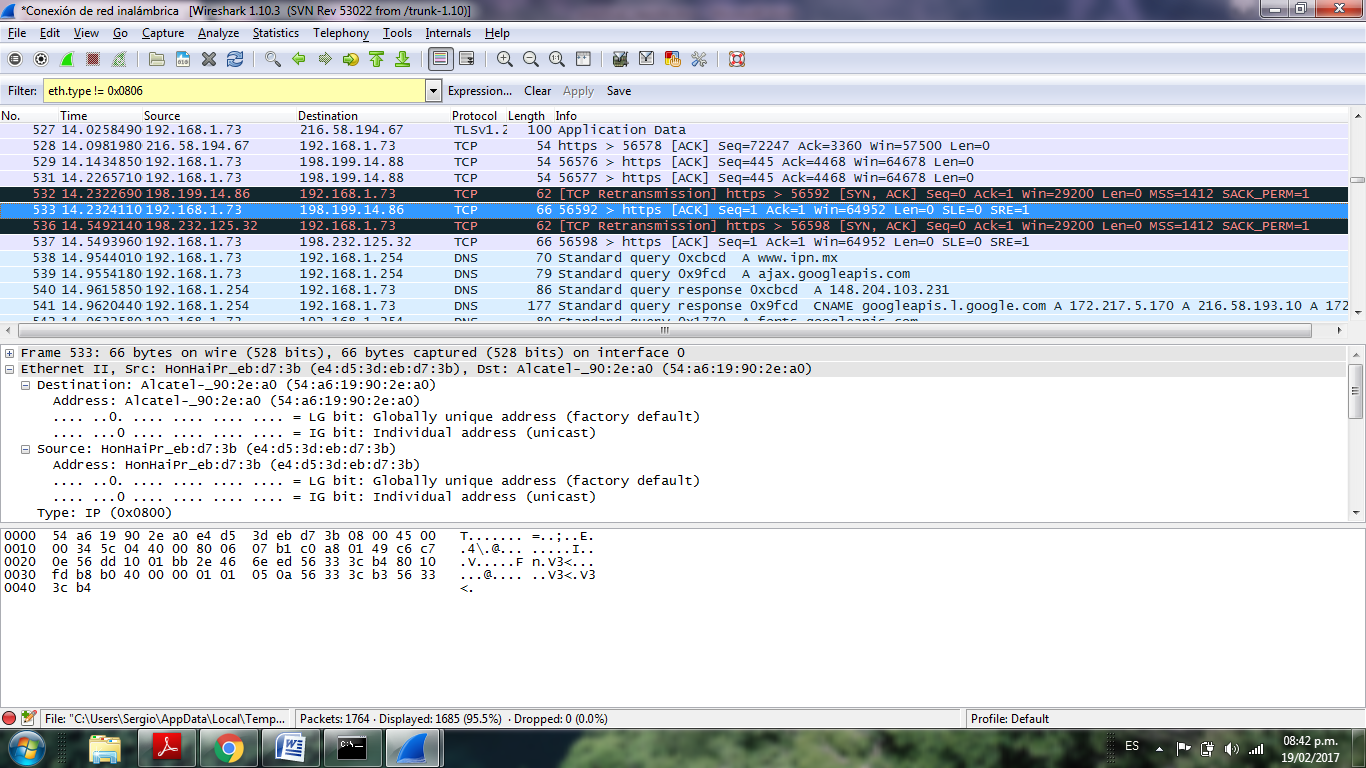
* Protocolo: ARP
* **Buscar dos tramas con distinto contenido en el campo tipo de la trama Ethernet (Ethertype), buscar el significado de su contenido y anotarlo**:



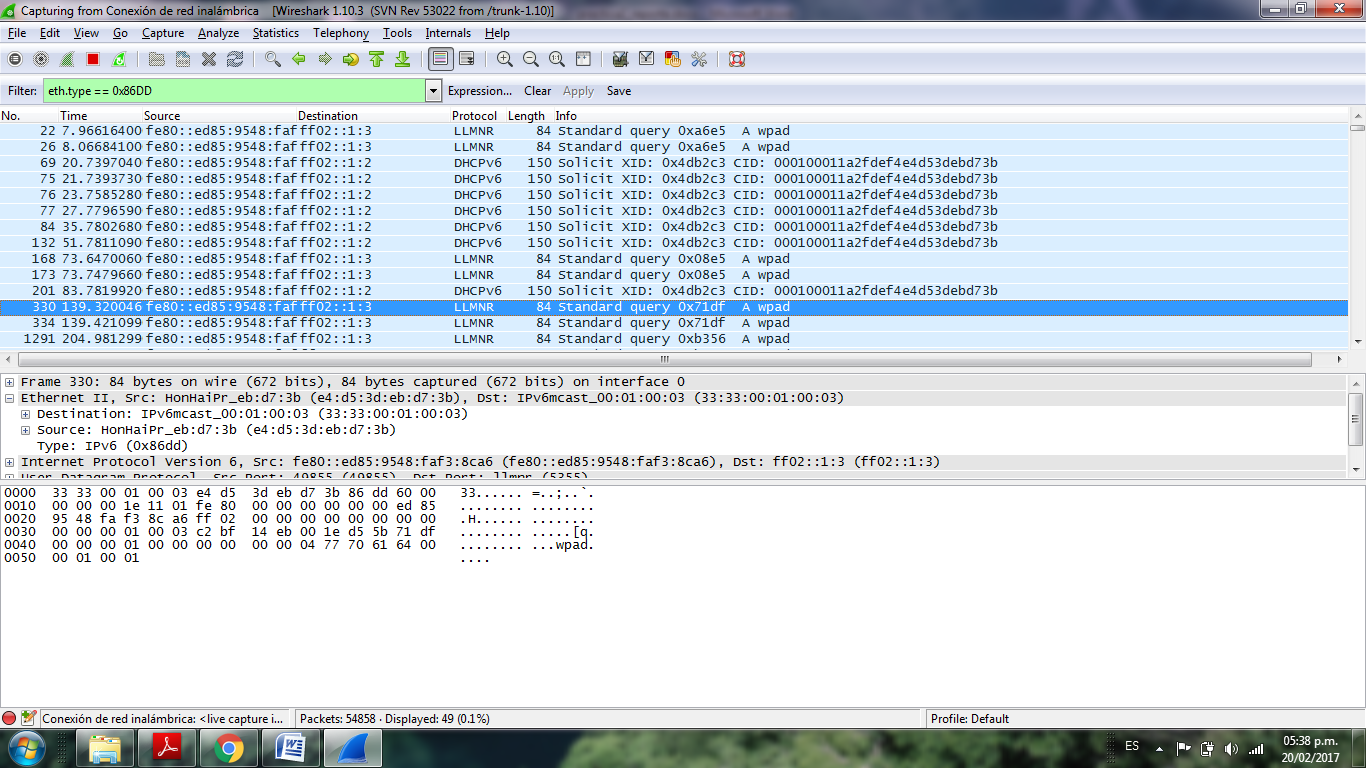
Ahora buscamos las tramas que contengan un contenido diferente en el campo de Ethertype.



1. Primer Trama:



1. Segunda Trama:



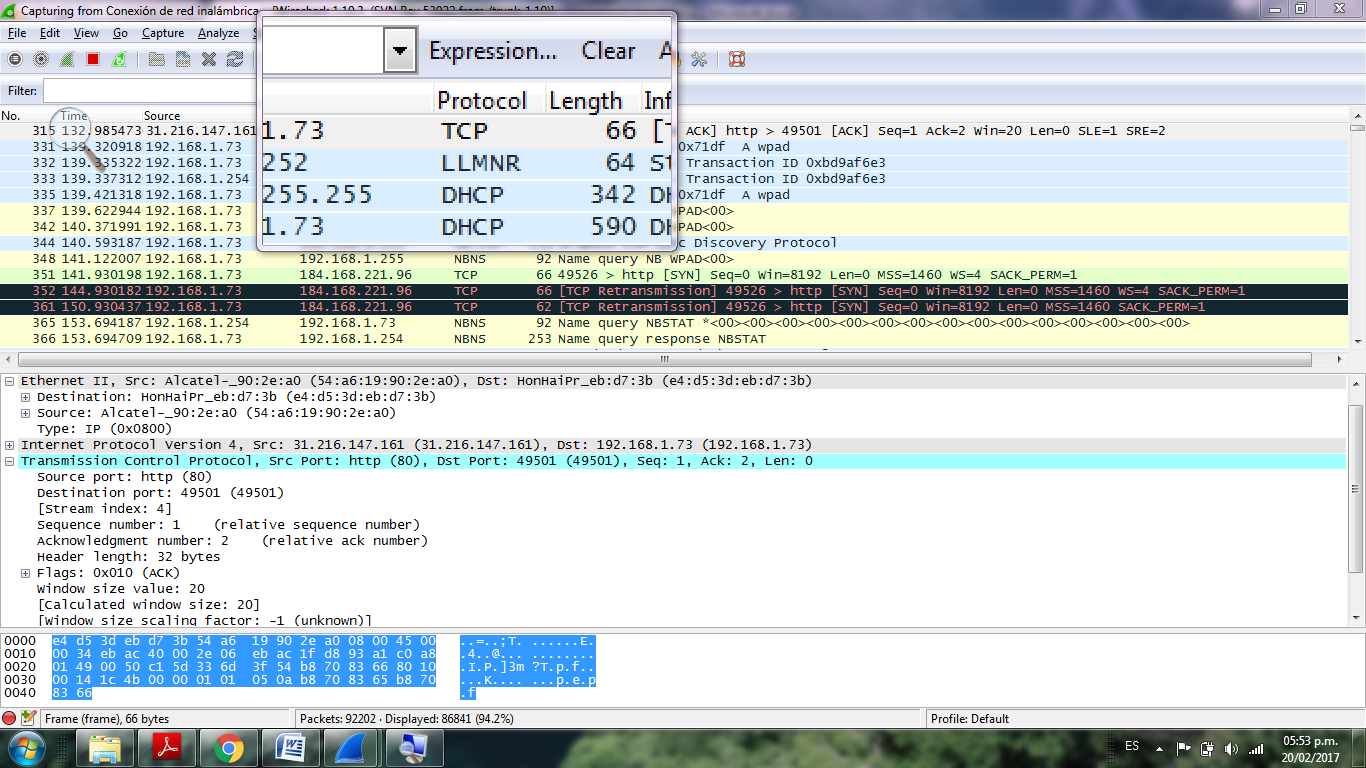
Protocolos encontrados diferentes de eth.type ¡= 0x0806

1. Primer Trama : TCP = 0x0800
2. Segunda Trama: LLMNR = 0x86DD

* **Identifique dos tramas que incluyan el protocolo IP y que tengan en su campo de protocolo destino, contenido diferente.**

Protocolo

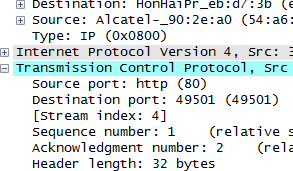
1. Pimer Trama:

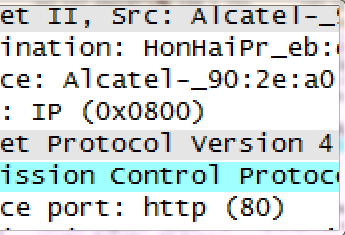
****

Puerto Destino: (49501)

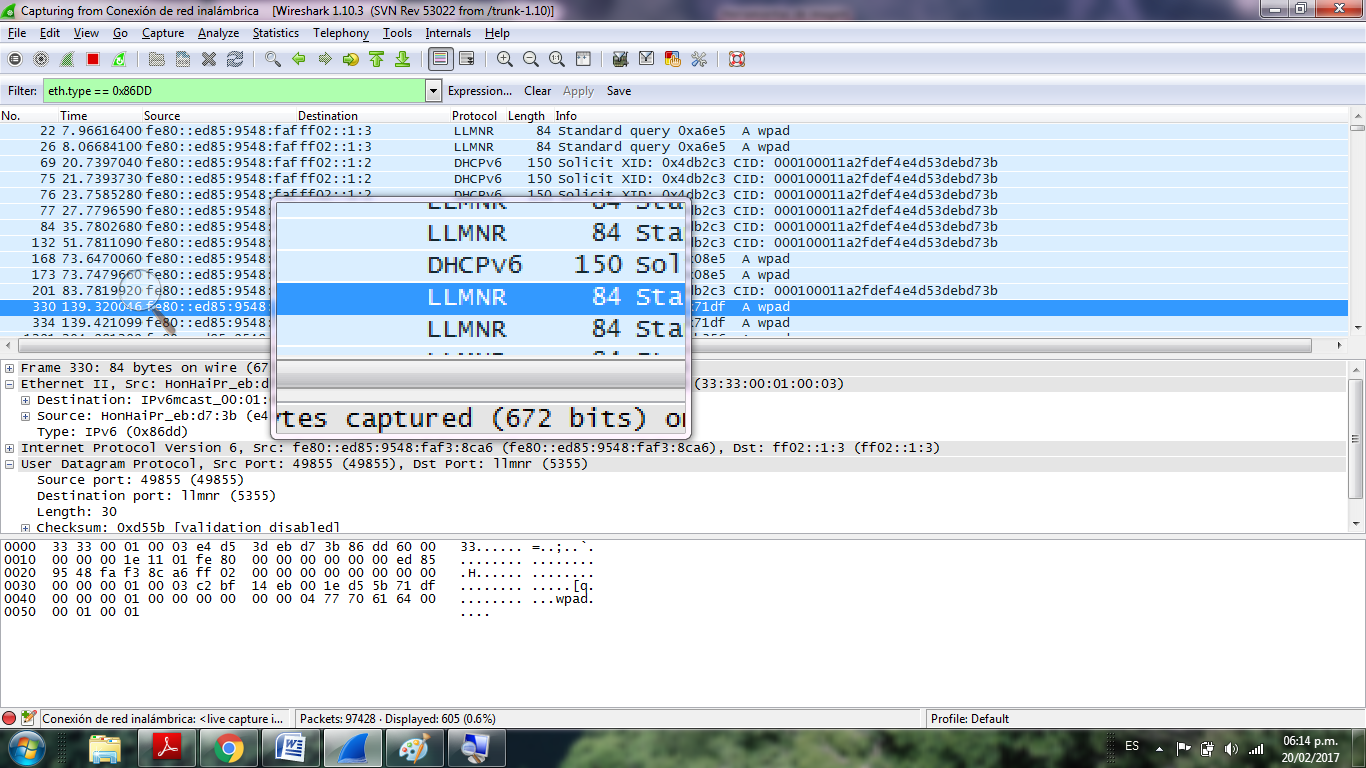
Formato Ethertype:

0x0800 = IPv4

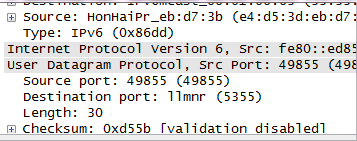




1. Segunda Trama: Protocolo

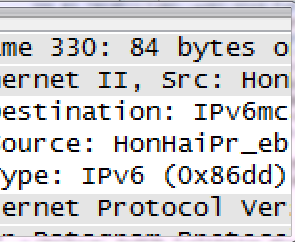


Puerto Destino: (5355)



Formato Ethertype:

0x86DD = IPv6

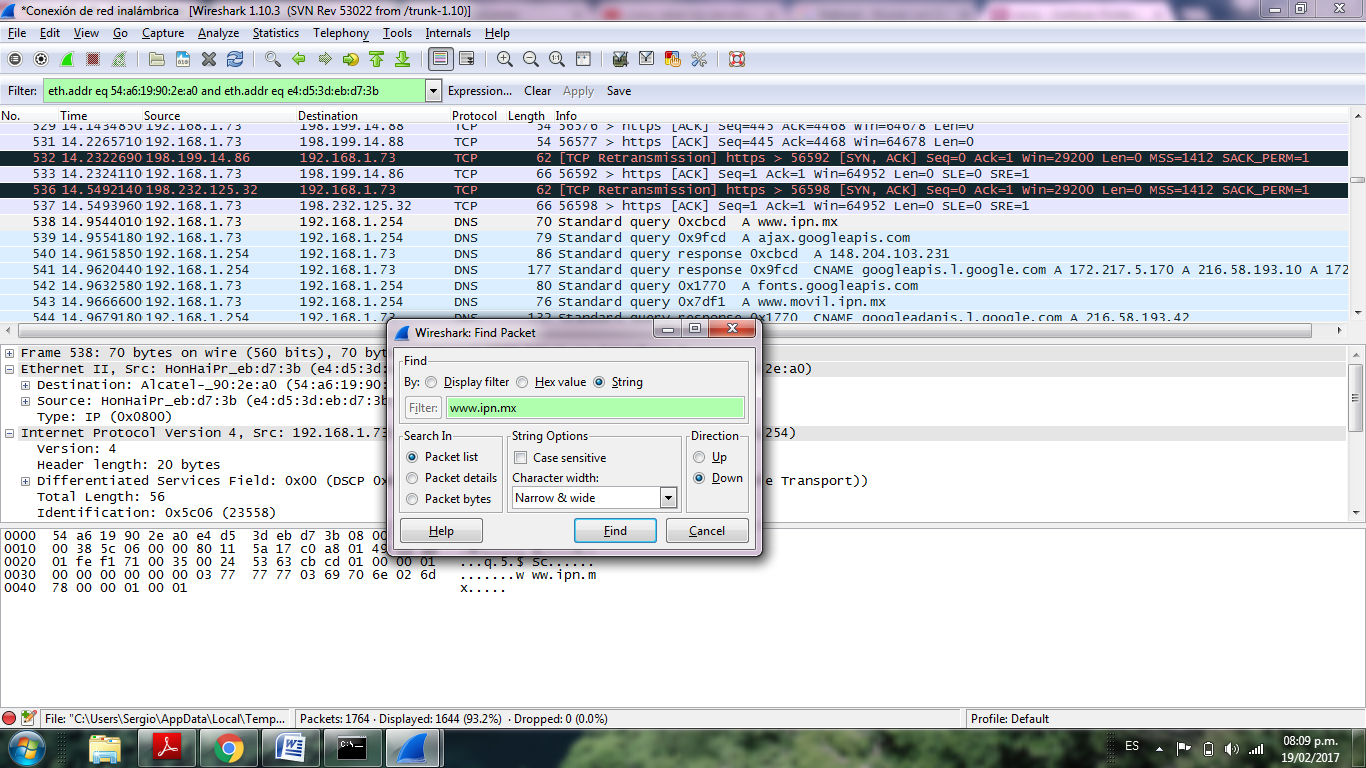


Comentario:

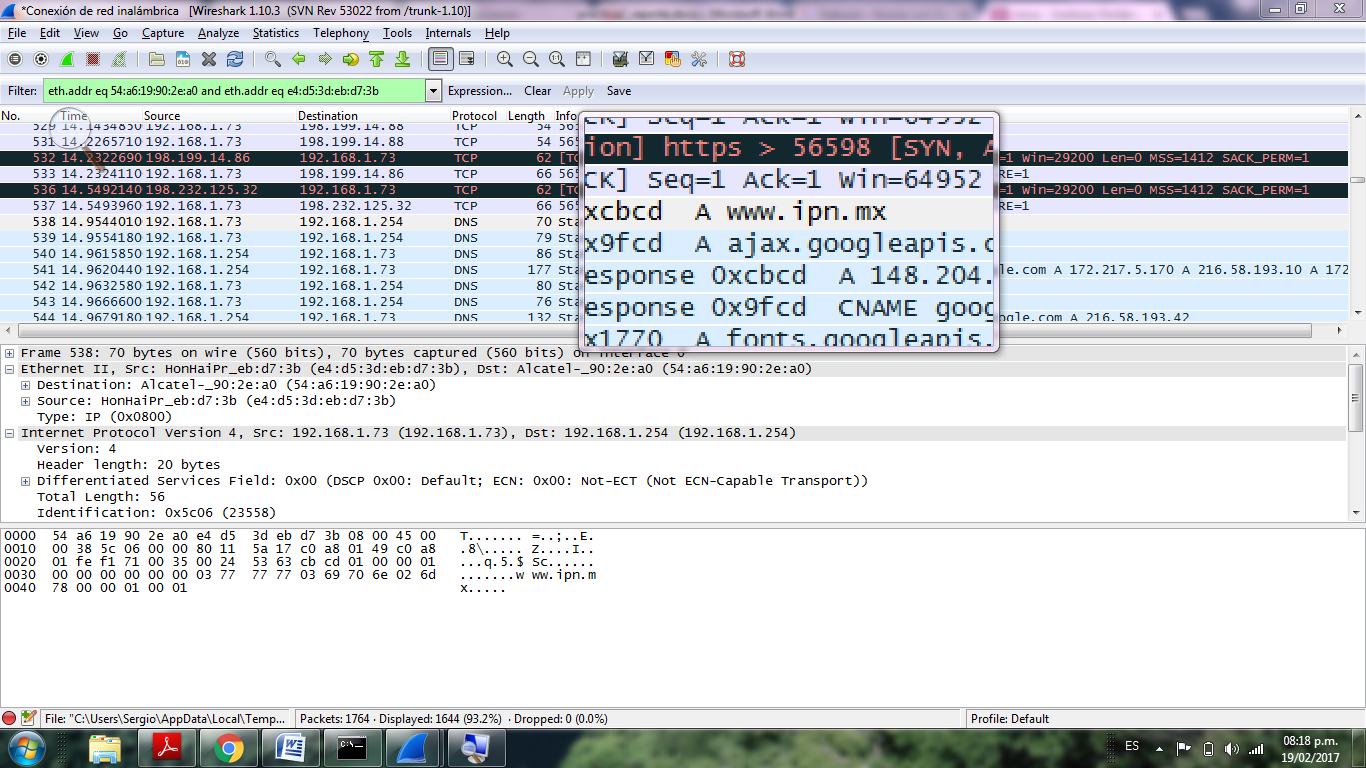
El protocolo IP está en la capa de red el cual ayuda a re direccionar o identificar a una maquina dependiendo la dirección IP y le transfiere datos por medio del protocolo TCP que está en la capa de transporte, esto es muy importante ya que en la familia TCP/IP son utilizadas o tambien de otra forma se podrían usar diferentes protocolos de red ya sea ARP o inclusive ICMP.

* **Buscar una trama donde aparezca www.ipn.mx y anotar los protocolos encapsulados en la misma.**

Después buscamos la trama en donde aparezca la página del IPN “www.ipn.mx”, y lo buscamos para ver, cuál es la trama que lo contiene (ver imágenes):



En la siguiente imagen se muestra la trama que contiene la página [www.ipn.mx](http://www.ipn.mx):



El protocolo que lo contiene es:

* DNS (Sistema de Nombres de Dominio)

**¿Cuáles son los protocolos orientados a conexión de la familia TCP/IP y como se inicia una conexión?**

Algunos protocolos orientados a conexión son:

* **TCP**: ¿Cómo se realiza la conexión?

En el TCP se establecen las conexiones usando el protocolo de acuerdo a tres vias (three-way handshake). Para establecer una conexión, un lado, digamos el servidor, espera pasivamente una conexión entrante ejecutando las primitivas LISTEN y ACCEPT y especificando cierto origen o bien nadie en particular.

En el otro lado, digamos el cliente, ejecuta una primitiva CONNECT especificando la dirección y el puerto IP con el que se desea conectar, el tamaño máximo de segmento TCP que está dispuesto a aceptar y opcionalmente algunos datos de usuario (ejemplo: contraseña). La primitiva CONNECT envía un segmento TCP con el bit SYN encendido y el bit ACK apagado, y espera una respuesta.

Al llegar el segmento al destino, la entidad TCP ahí revisa si hay un proceso que haya ejecutado un LISTEN en el puerto indicado en el campo de *puerto de destino*. Si no lo hay, envía una contestación con el bit RST encendido para rechazar la conexión.

Si algún proceso está escuchando en el puerto, ese proceso recibe el segmento TCP entrante y puede entonces aceptar o rechazar la conexión; si la acepta, se devuelve un segmento de acuse de recibo.

* **Frame Relay**: ¿Cómo se realiza la conexión?

• Cada router es conectado al Switch Frame Relay por medio de un CSU/DSU.

• El router indaga el estado del circuito virtual.

• Cuando el Switch Frame Relay recibe la petición responde informando los DLCI locales de los PVC a los routers remotos.

• Por cada DLCI activo los routers envían un paquete ARP inverso que contiene la dirección IP correspondiente a cada Circuito Virtual.

• Los routers remotos crean tablas que incluyen los DLCI locales y las direcciones IP.

• Cada 60 segundos se envían los mensajes ARP inverso.

• Cada 10 segundos se intercambia información LMI.

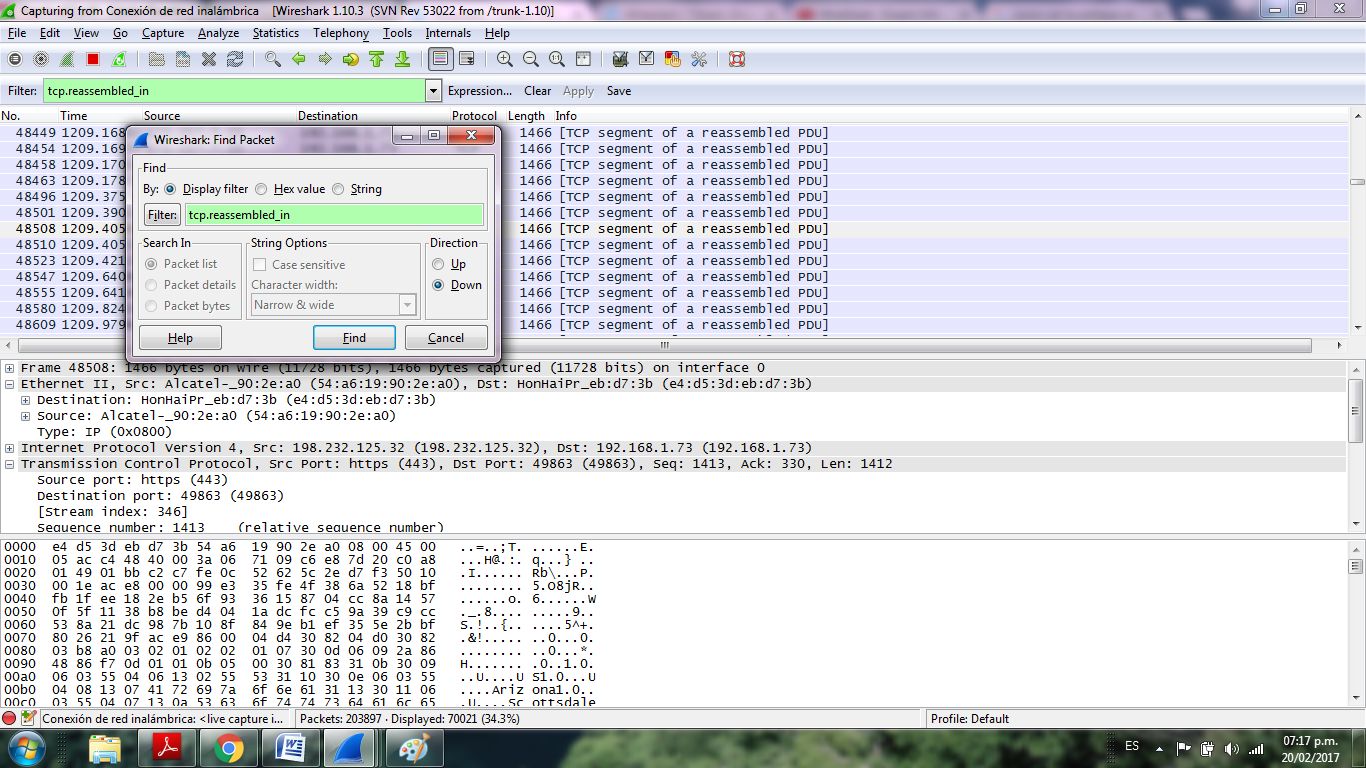
* **ATM**: ¿Cómo se realiza la conexión?

Una conexión ATM, consiste de "celdas" de [información](http://www.monografias.com/trabajos7/sisinf/sisinf.shtml) contenidos en un circuito virtual (VC). Estas celdas provienen de diferentes [fuentes](http://www.monografias.com/trabajos10/formulac/formulac.shtml#FUNC) representadas como generadores de bits a tasas de transferencia constantes como la voz y a tasas [variables](http://www.monografias.com/trabajos12/guiainf/guiainf.shtml#HIPOTES) tipo ráfagas (bursty traffic) como los datos. Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para trasiego de información y los restantes para uso de campos de [control](http://www.monografias.com/trabajos14/control/control.shtml) (cabecera) con información de "**quién soy**" y "**donde voy**"; es identificada por un "virtual circuit identifier" VCI y un "virtual path identifier" VPI dentro de esos campos de control, que incluyen tanto el enrutamiento de celdas como el tipo de conexión. La [organización](http://www.monografias.com/trabajos6/napro/napro.shtml) de la cabecera (header) variará levemente dependiendo de sí la información relacionada es para interfaces de red a red o de usuario a red. Las celdas son enrutadas individualmente a través de los conmutadores basados en estos identificadores, los cuales tienen significado local - ya que pueden ser cambiados de interface a interface.

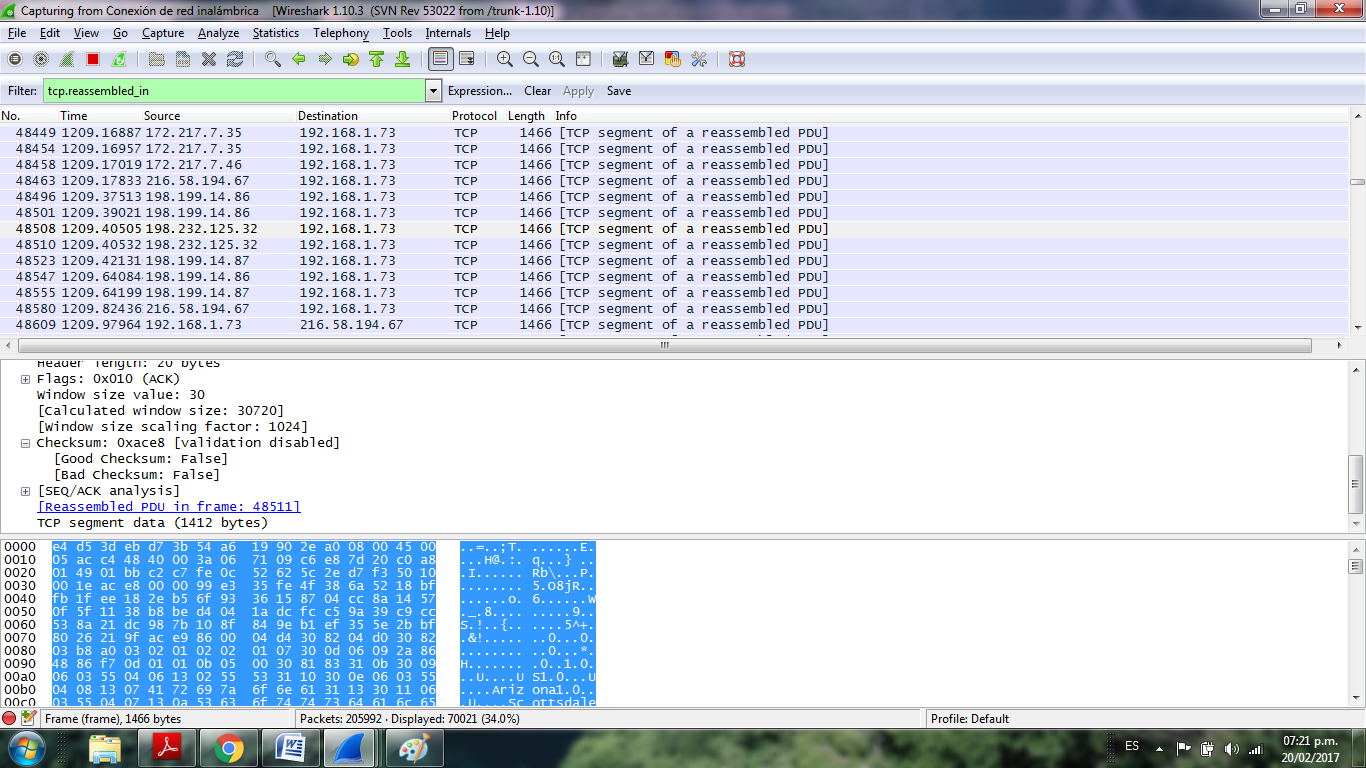
**Anote el nombre de algún campo que tenga que ver con:**

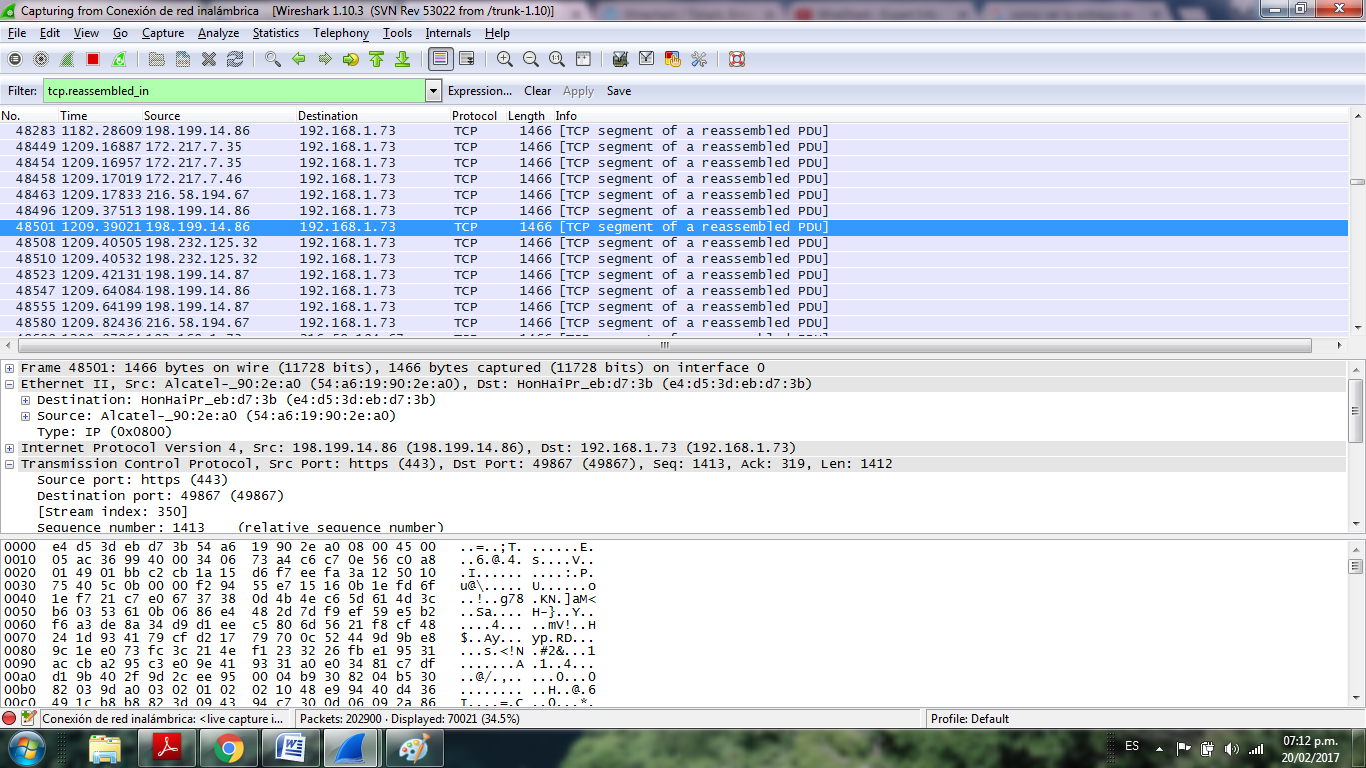
1. **La entrega en orden**
2. **La segmentación (fragmentación) dentro del protocolo IP**
3. **El control de error**

Tenemos una captura cualquiera con algunas etiquetas de información del tipo **TCP segment of a reassembled PDU**, no sabemos a cuantos paquetes afecta esta información, error o lo que sea, así que aplicamos un Display Filter:

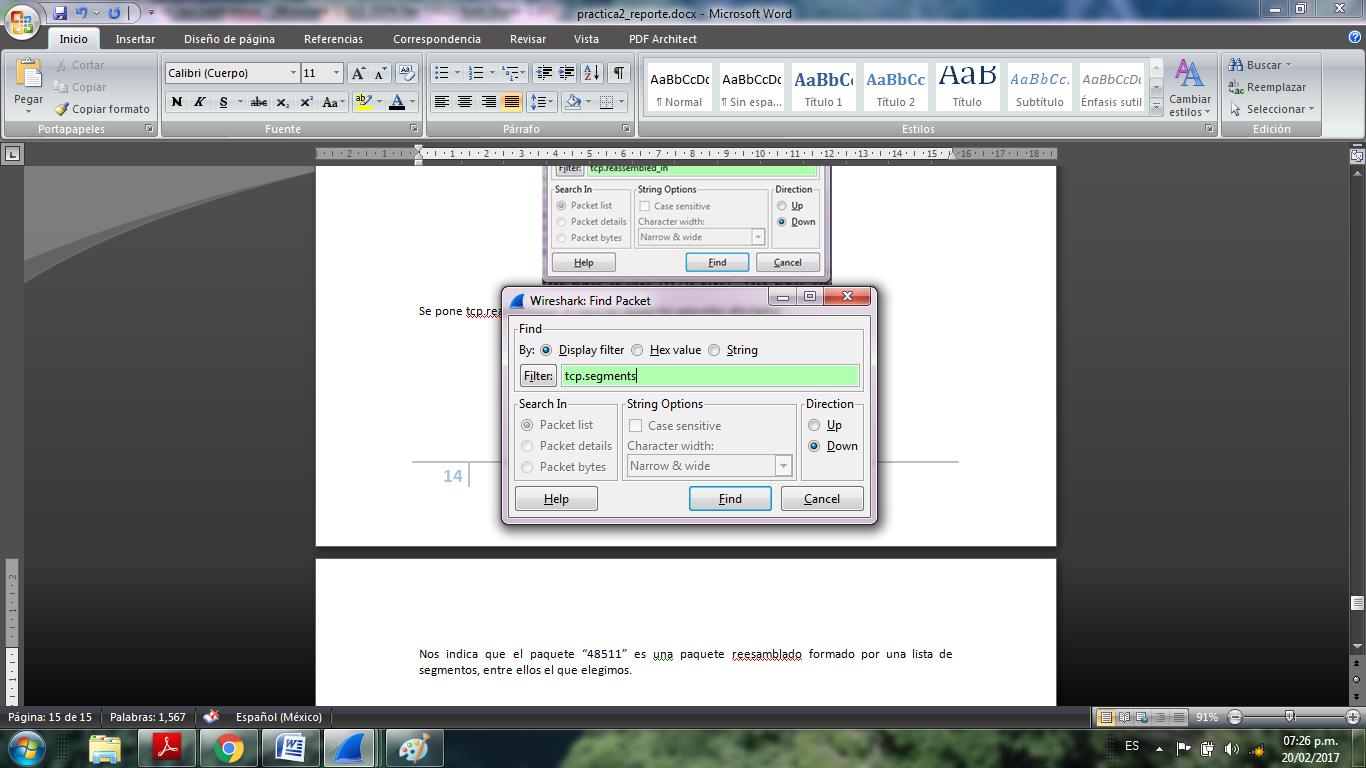


Se pone tcp.reassembled\_in para ver todos los paquetes afectados:

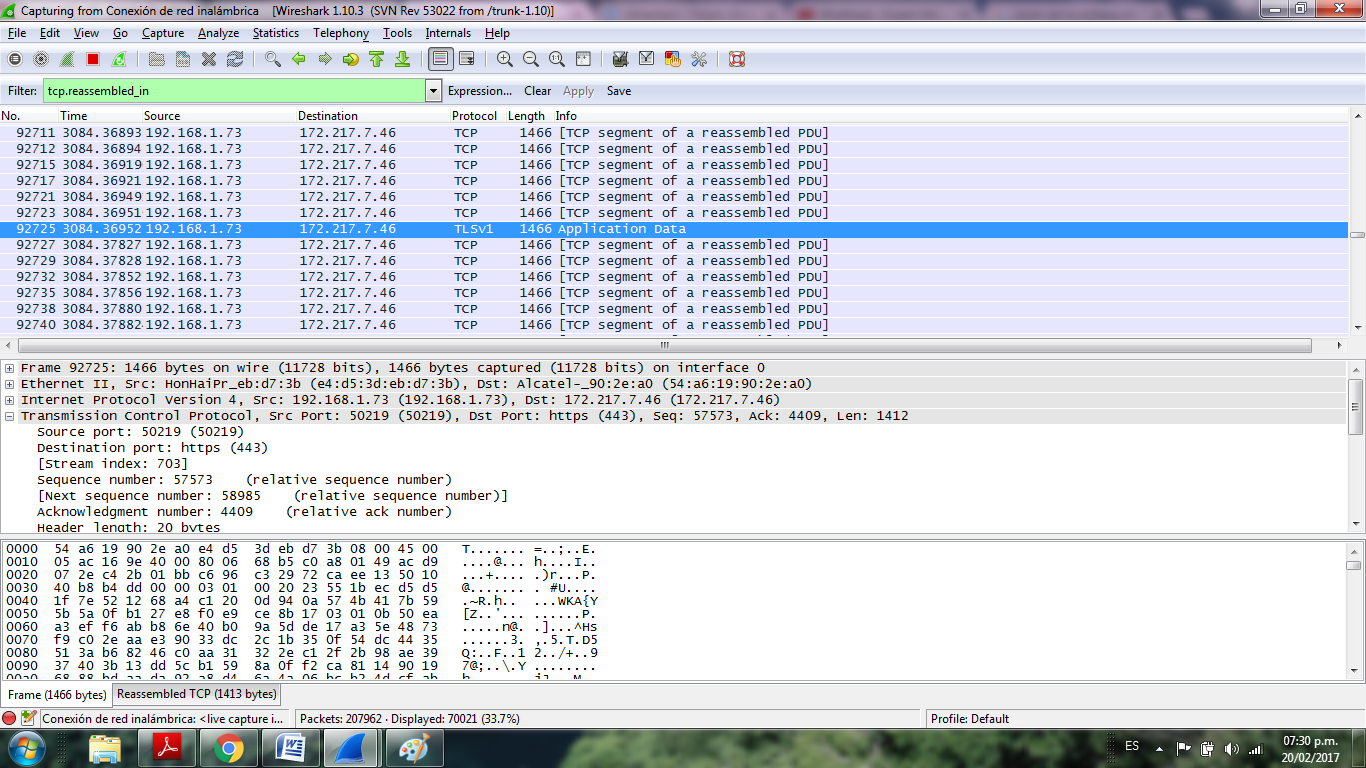




Nos indica que el paquete “48511” es una paquete resemblado formado por una lista de segmentos, entre ellos el que elegimos.



Ponemos en buscar filtro “tcp.segments” para que busquemos los segmentos re ensamblados.



Esta búsqueda nos dice que el paquete a concatenado una serie de segmentos mostrando en él toda la información completa.

En ocasiones, nos encontramos una serie de errores que por su número y/o descripción parece que tenemos un problema grave en un **host** o en la **red**.

Información de Error:



Podemos observar que en donde tenemos el protocolo Ethernet tenemos un problema de Bad checksum.

En la gran mayoría de implementaciones de la pila de protocolos el checksum de los [segmentos TCP](https://seguridadyredes.wordpress.com/2008/01/29/analisis-capturas-trafico-de-red-interpretacion-segmento-tcp-ii-establecimento-conexian-tcp) o [datagramas UDP](https://seguridadyredes.wordpress.com/2008/02/06/analisis-capturas-trafico-de-red-interpretacion-datagrama-udp-iii) salientes no los realiza la CPU. Esta función está encomendada a la tarjeta de red. Esto es así para reducir la carga de la CPU y que de esta forma aumente el rendimiento de host.