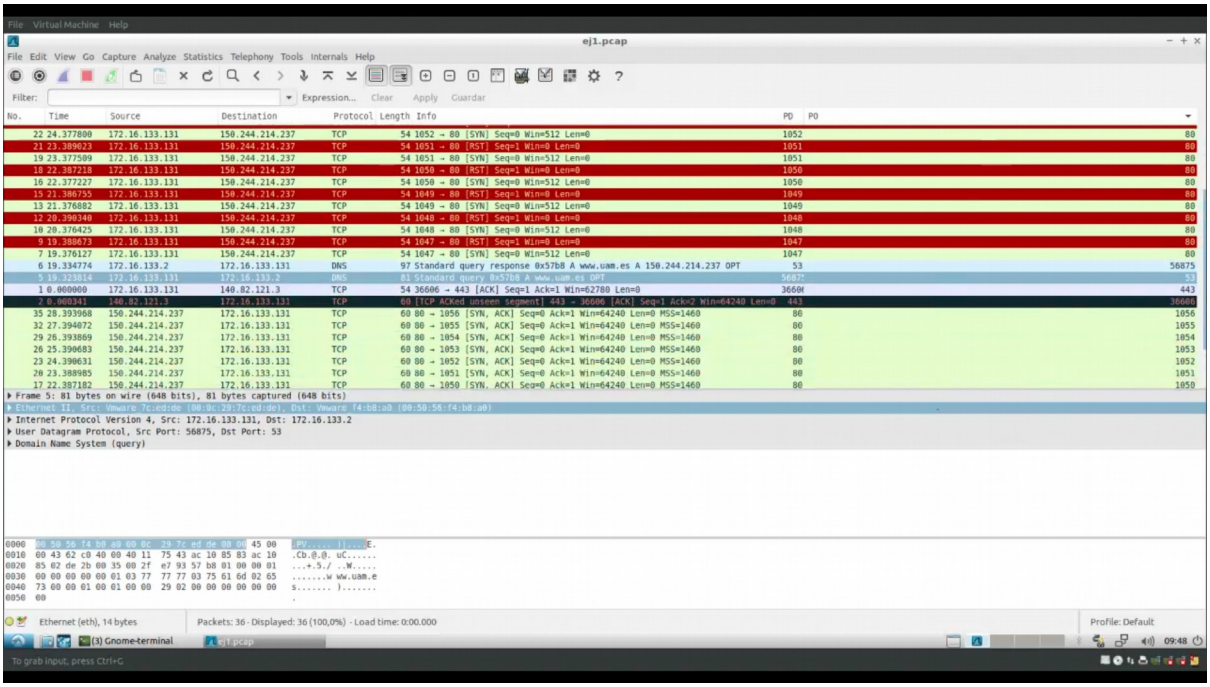
Ejercicios Wireshark:

Angel Casanova Bienzobas y Rodrigo Juez Hernández

Ejercicio 1:

El proceso seguido ha sido el del ejercicio, abrimos wireshark y hicimos ping a la web de la UAM, tuvimos un único problema y es que las columnas PO y PD no se veían debido a que el campo “Info” era muy largo.
Del análisis solo sacamos en claro que los paquetes eran de longitud corta, entre 50-70 llegando en muy pocos a 100.
Solo había un **único** paquete con el número **53** en el campo PO.



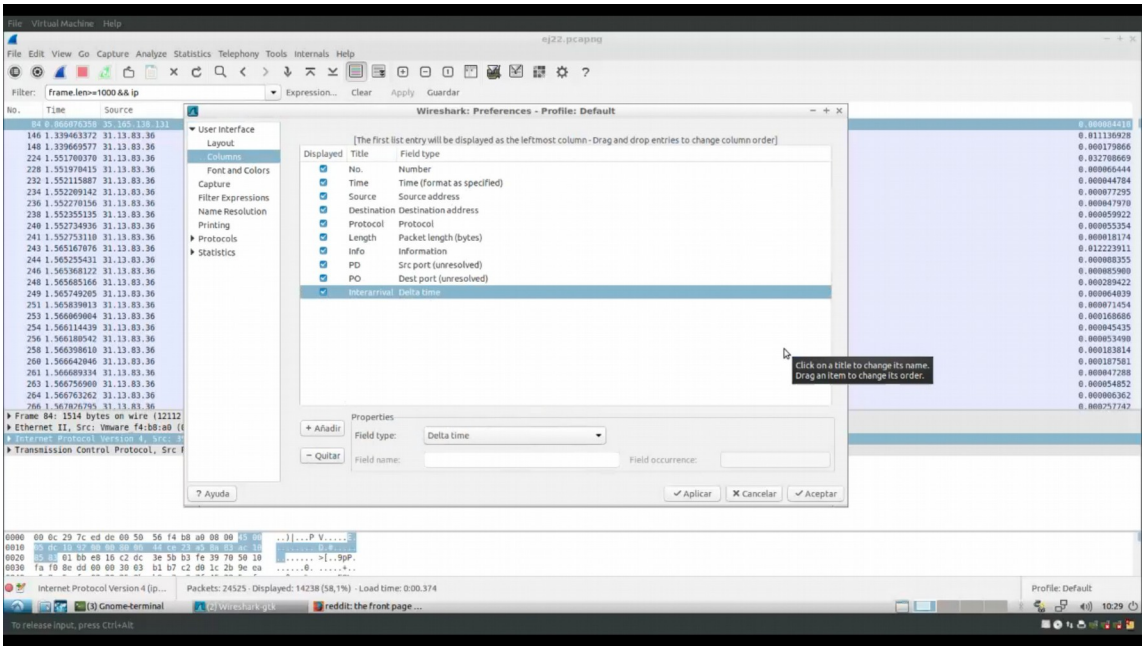
Ejercicio 2:

1. frame.len>=1000 && ip
2.
    a. Edit-> Mark All Displayed Plackets
    b. Export Specified Packets…
    c. Click on Marked packets only
    d. Save with format .pcap
3. Observamos que la longitud de la IP es siempre 14 menos que la longitud del paquete.

IP Length	Length
1488	1502
1488	1502
1091	1105
1488	1502
1500	1514

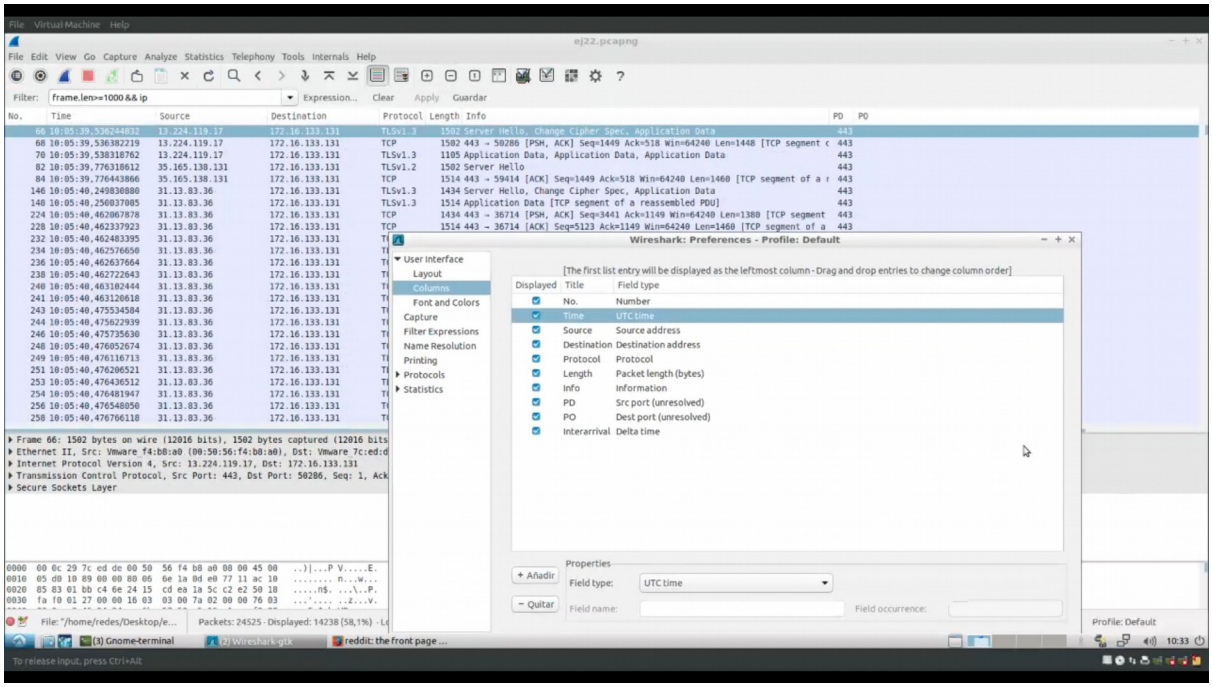
Ejercicio 3:

Edit -> Preferences -> User Interface -> Columns -> Add... -> Field Type = Delta Time

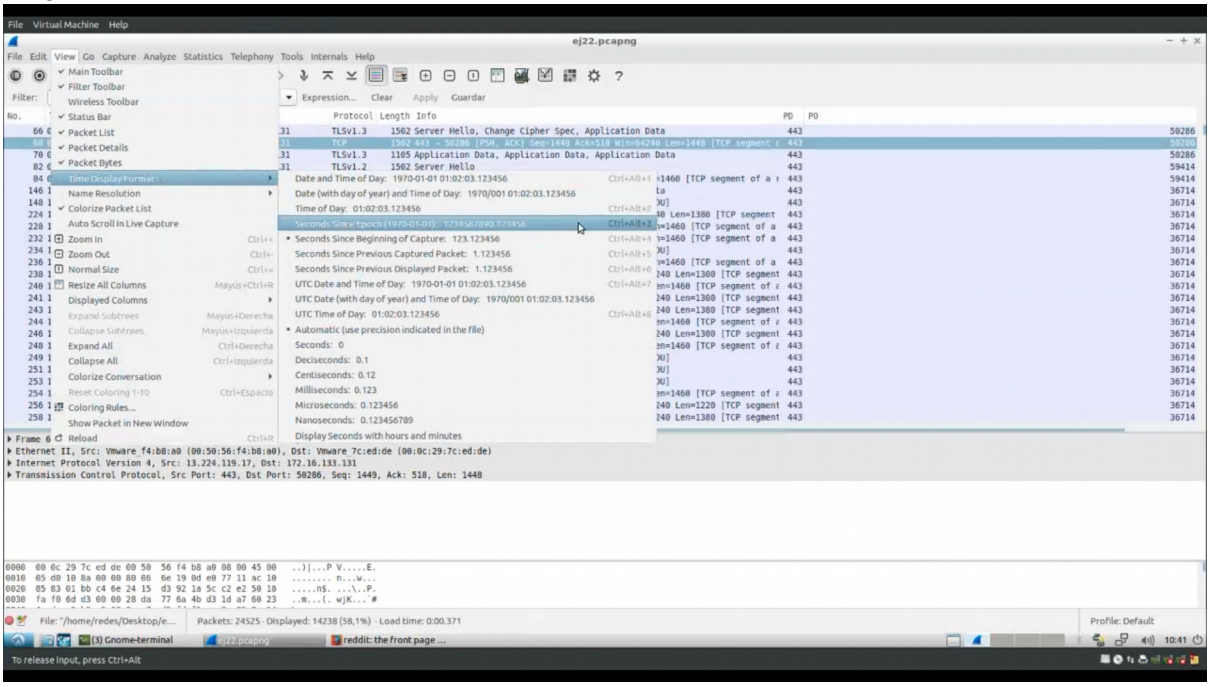


Ejercicio 4:

Tiempo para humanos (UTC Time): Modificamos la columna time a UTC dado que España usa UTC +1 y era lo más humano posible.



Tiempo UNIX:
Los pasos a seguir son: View -> Time Display Format -> Seconds since Epoch
UNIX mide el tiempo como los segundos desde el 1 de Enero de 1970, igual que lo que hemos elegido.



Ejercicio 5:

Se selecciona la interfaz “ens33” y se usa la opción configurar, ahí en la sección **Capture Filter** escribimos **udp** y damos a Start, navegamos y hacemos ping a la UAM y detuvimos la captura. Observamos que todos los paquetes son DNS y podemos comprobar que son UDP haciendo click y en la pestaña User Datagram Protocol que efectivamente es UDP.