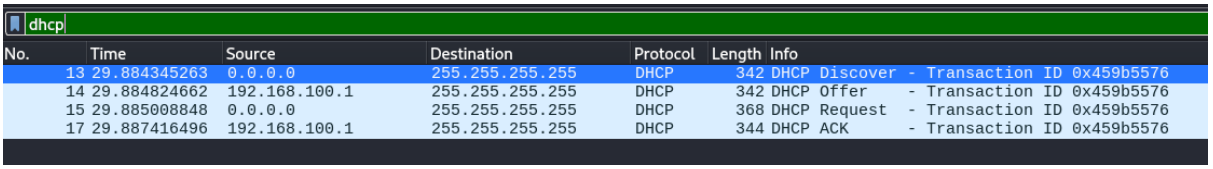
Análisis del Tráfico DHCP con Wireshark

Vamos a analizar el tráfico DHCP que hay entre un cliente y un servidor cuando este ultimo quiere conectarse a la red.

Tenemos instalado un Windows server que nos esta sirviendo de servidor DHCP, con una pool que abarca entre 192.168.100.10 y 192.168.100.25.
Tenemos además un cliente al cual vamos a borrar y renovar su configuración de adaptador de red para simular que es un equipo que nunca se ha conectado a la red previamente.
Tambien borraremos la entrada de la concesión de la ip para la mac del cliente en el servidor, asi podremos analizar el proceso de configuración dinamica al completo.

1. Borramos la configuración de red con ipconfig /release, y la renovamos con ipconfig /renew para que el cliente vuelva a solicitar una nueva dirección ip al servidor DHCP.

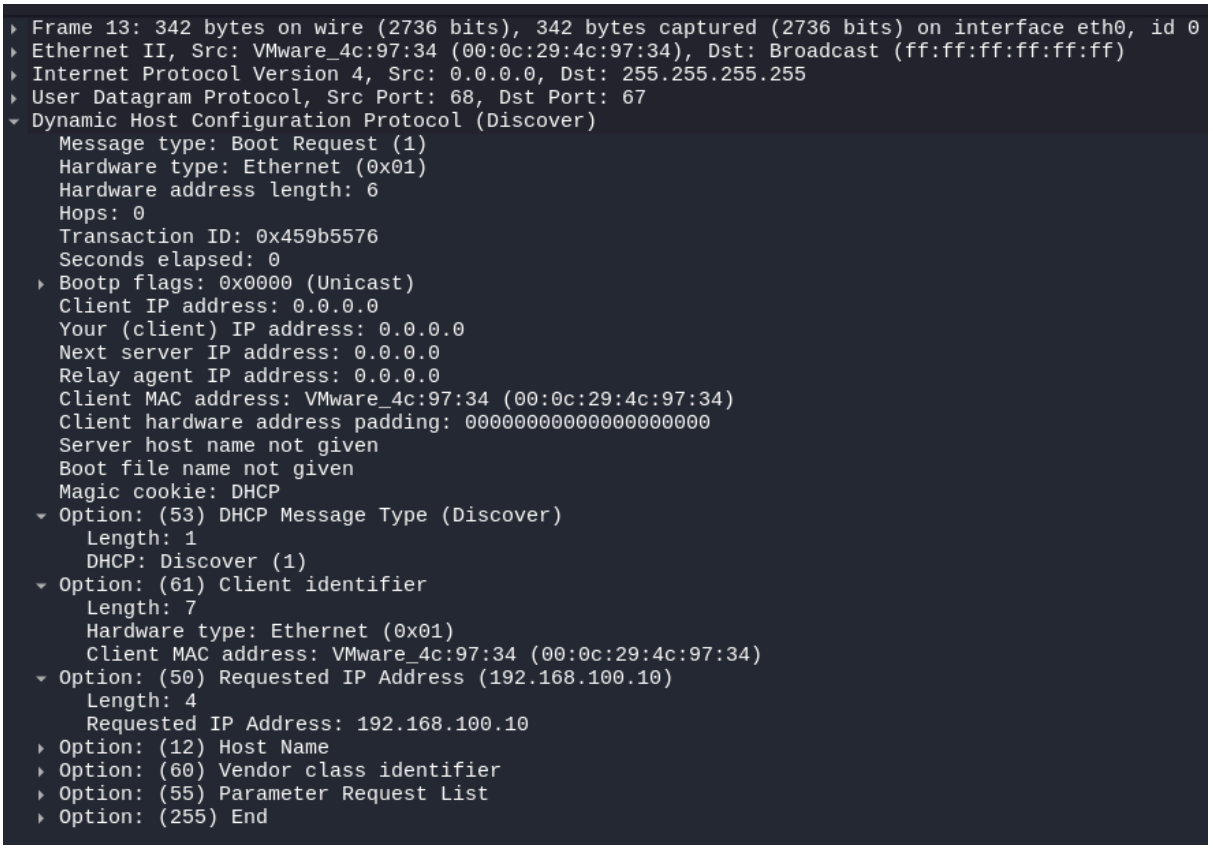
2. En una segunda maquina conectada a la red tenemos abierto wireshark para capturar los paquetes que se mueven en ella. Filtramos por DHCP, y una vez lanzamos ipconfig /renew en el cliente empezamos a capturar paquetes del protocolo.
   Podemos observar 4 paquetes:
   a. DISCOVER: Se envia del cliente (temporalmente 0.0.0.0) al broadcast, ya que no conoce la red, de esa manera llegara a cualquier equipo dentro de ella, para descubrir si hay algun servidor dhcp.
   b. OFFER: Lo manda el servidor nuevamente al broadcast, ya que el cliente aun no tiene IP, ofreciendole una de las direcciones disponibles dentro de la pool.
   c. REQUEST: Lo manda el cliente al broadcast, solicitando la IP que le ha ofrecido el servidor.
   d. ACK: Finalmente se termina la transacción con un paquete del servidor al broadcast, “reconociendo” que la dirección IP sugerida se asociara con la MAC del cliente para llevar a cabo la configuración automatica.



Paquete Discover

Podemos encontrar:

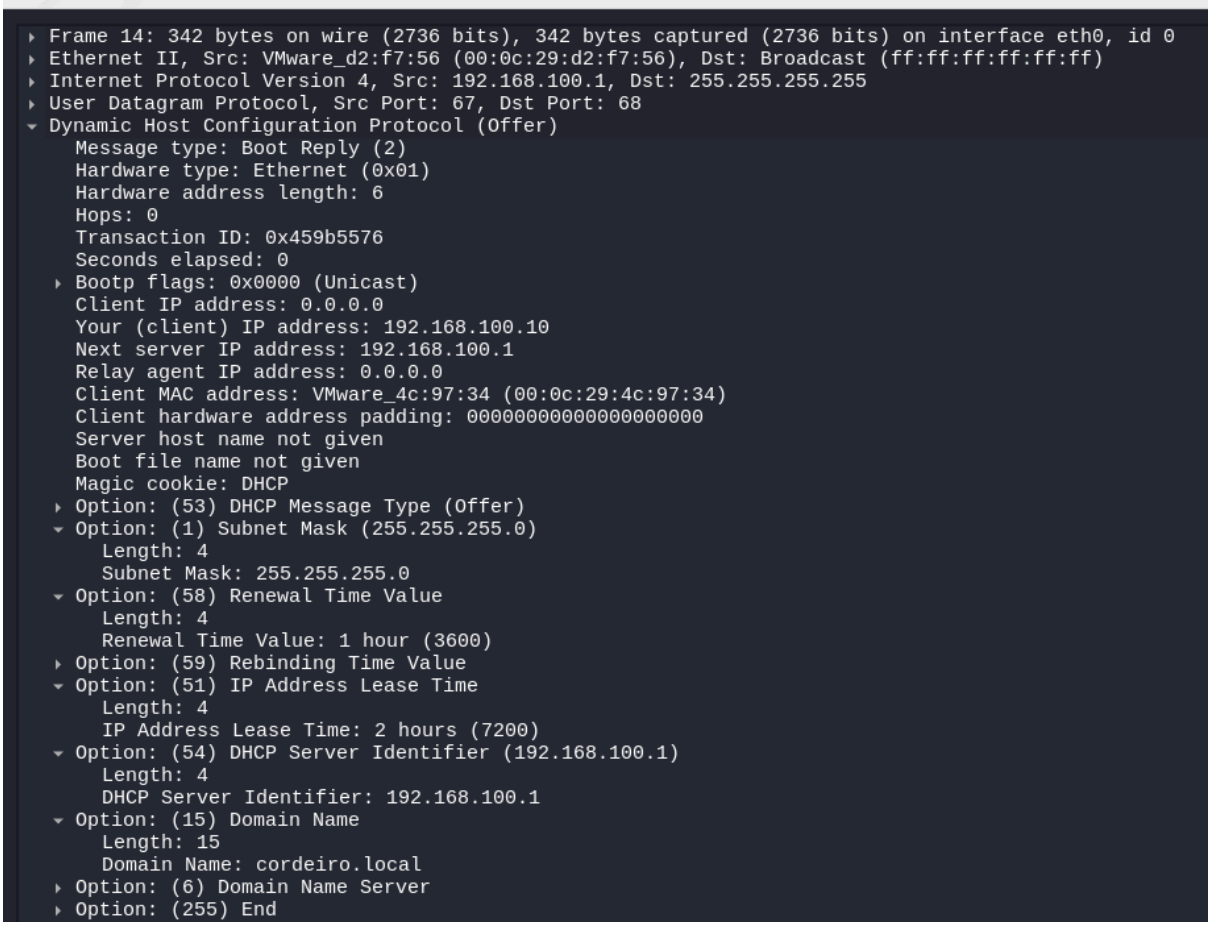
- El tipo de paquete dentro del protocolo DHCP, Discover.
- IP del cliente: 0.0.0.0.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP solicitada: 192.168.100.10, su anterior dirección, probablemente porque quede algun dato en caché.



Paquete Offer

Podemos encontrar:

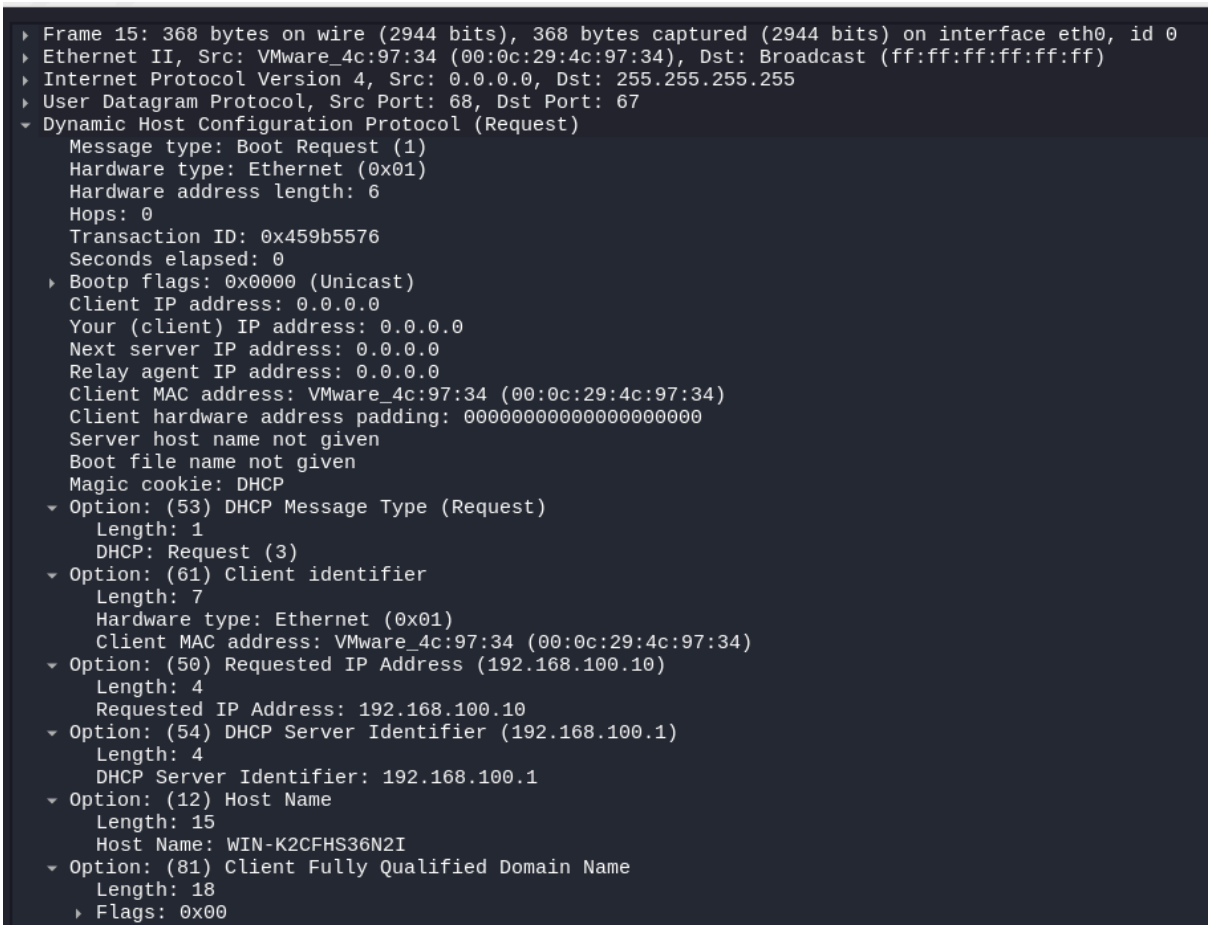
- El tipo de paquete dentro del protocolo DHCP, Offer.
- IP del cliente: 192.168.100.10, la que le esta ofreciendo.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP ofrecida: 192.168.100.10, la primera disponible en la pool.
- Mascara de subred: 255.255.255.0.
- Lease: 2h.
- Dirección del servidor DHCP: 192.168.100.1.
- Nombre de dominio del servidor: cordeiro.local.



Paquete Request

Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, request.
- IP del cliente: 0.0.0.0, aún sin IP
- MAC del cliente: 00:0c:29:4c:97:34.
- IP solicitada: 192.168.100.10, la ofrecida por el servidor.
- Dirección del servidor DHCP: 192.168.100.1.
- Nombre de equipo del servidor: WIN-K2CFHS36N2I.



Paquete ACK

Podemos encontrar:

- El tipo de paquete dentro del protocolo DHCP, ACK.
- IP del cliente: 192.168.100.10, la ofrecida y solicitada, que se asignara en la tabla ARP a la MAC del cliente.
- MAC del cliente: 00:0c:29:4c:97:34.
- IP ofrecida: 192.168.100.10, la primera disponible en la pool.
- Mascara de subred: 255.255.255.0.
- Lease: 2h.
- Dirección del servidor DHCP: 192.168.100.1.