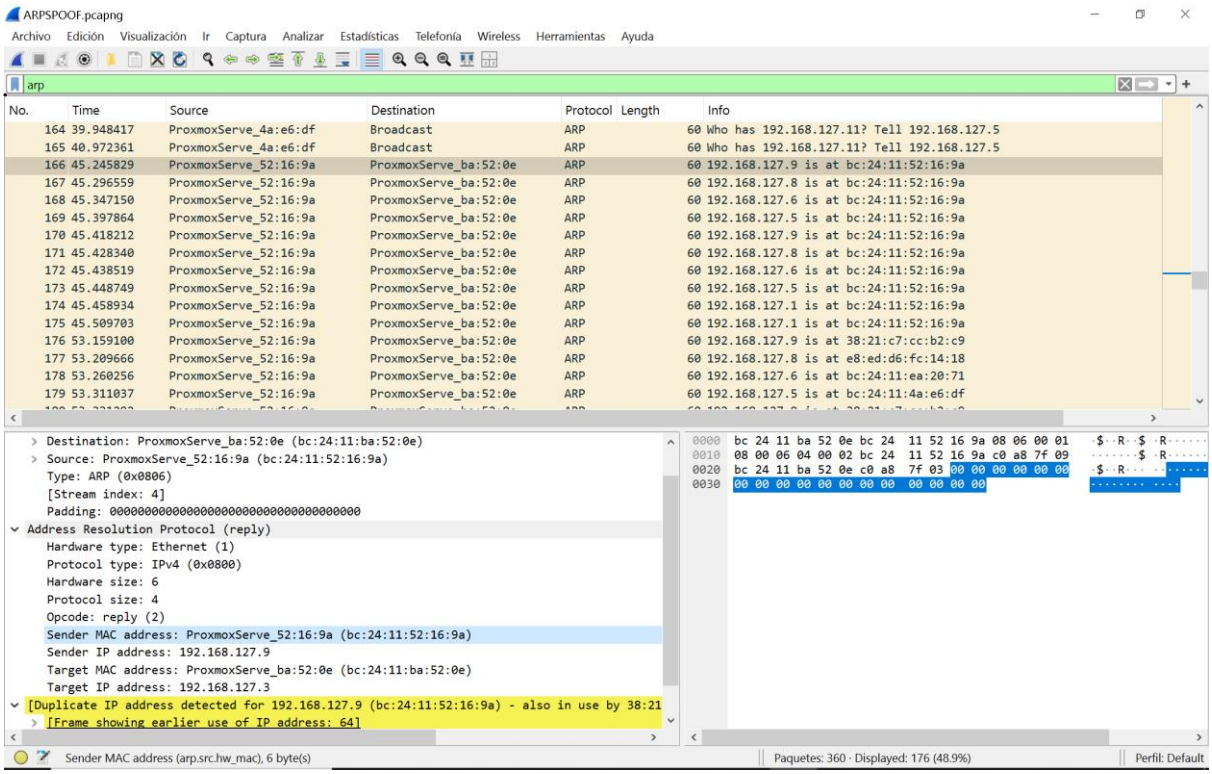
LABORATORIO
Analisis Forense con WireShark

Pregunta 1 : ¿Cual es la mac address del atacante?. Justifica con evidencia

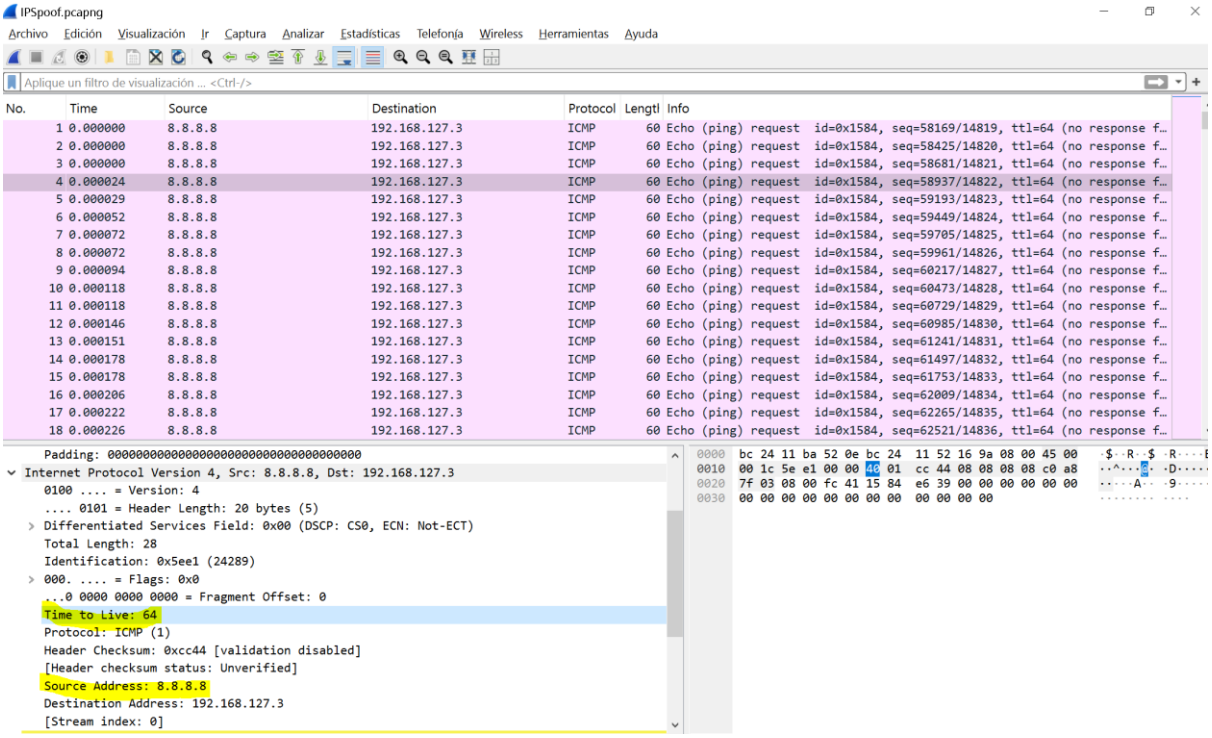
Captura ARPSPOOF.pcapng



R: La dirección MAC **bc:24:11:52:16:9a** puede ser identificada como la del atacante, ya que aparece en múltiples campos clave del tráfico de red, incluyendo el campo **"Source MAC Address"** y el campo **"Sender MAC Address"** en respuestas ARP. Además, la captura muestra una alerta de **conflicto de IP**, indicando que la IP **192.168.127.9** está siendo utilizada simultáneamente por dos direcciones MAC distintas: **bc:24:11:52:16:9a** y **38:21:c7:cc:b2:c9**. Este tipo de comportamiento es típico en ataques de **ARP poisoning**, donde un atacante intenta redirigir el tráfico de red hacia su dispositivo mediante la falsificación de respuestas ARP

Pregunta 2 : ¿Cual es el sistema operativo del atacante?. Justifica con evidencia

IPSpoof.pca.png



R: En este caso el TTL (**time tolive de 64**) indica que se trata de un sistema operativo Linux