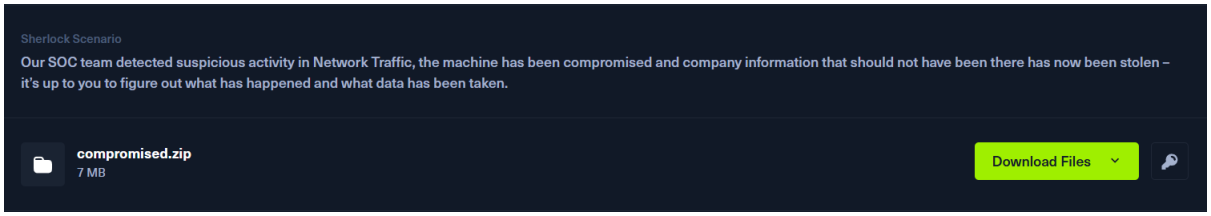
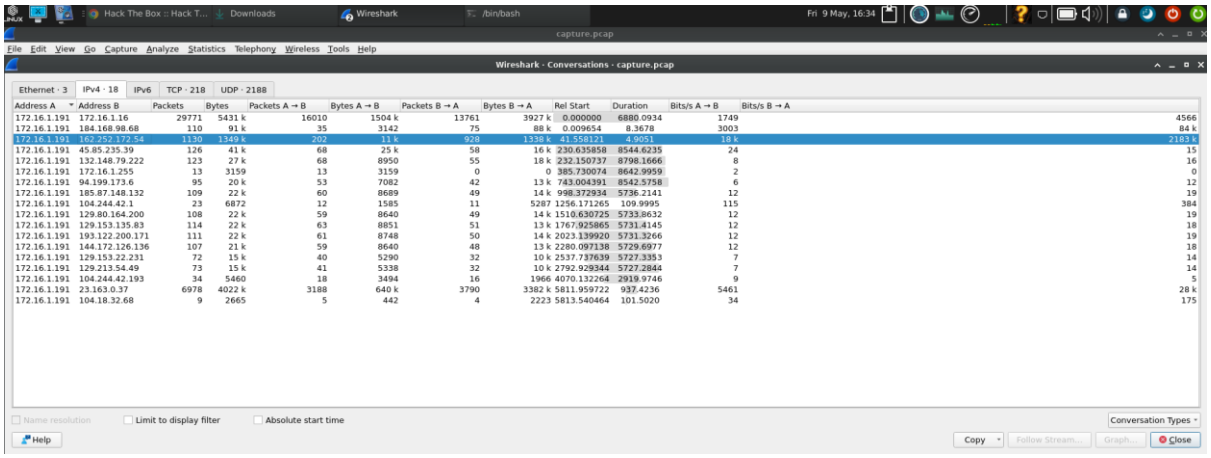
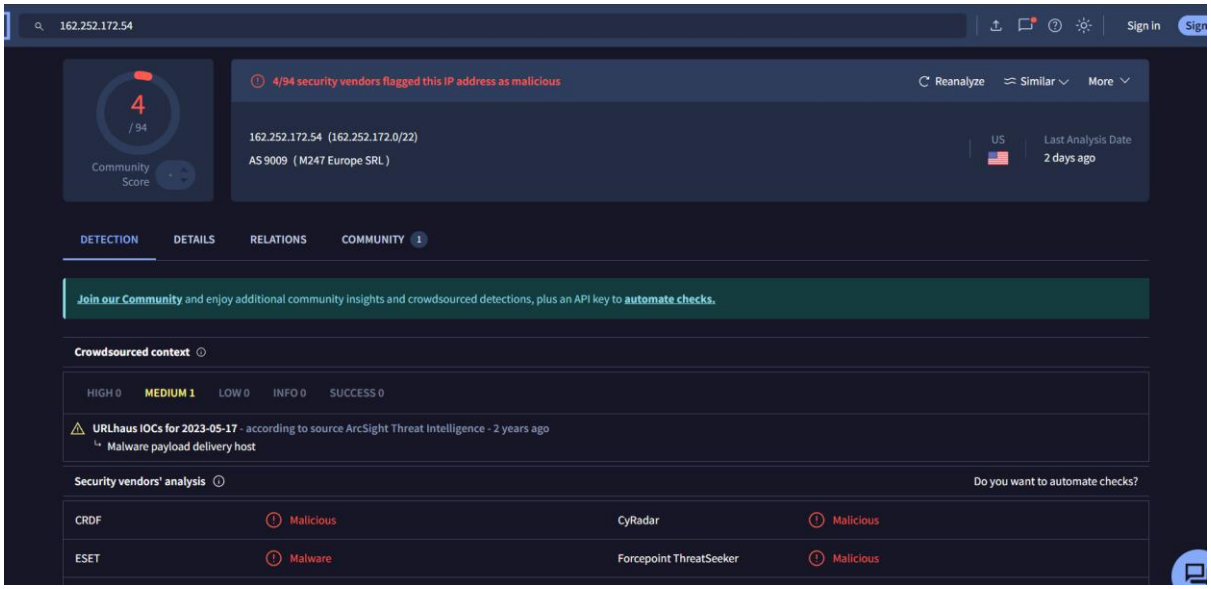


FLAG-1 IP sospechosa identificada

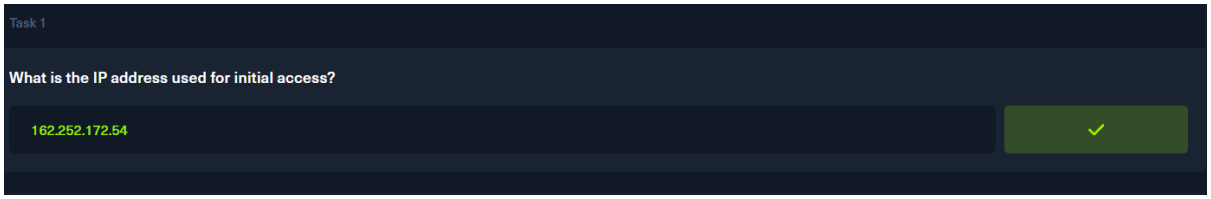
Para identificar la dirección IP sospechosa, accedí a la sección de **Conversaciones** en Wireshark, donde analicé el tráfico entre las diferentes direcciones IP activas en la red. Observando el volumen y comportamiento de los paquetes, detecté una IP que generaba ruido anómalo: `162.252.172.54`



Posteriormente, consulté esta IP en **VirusTotal**, donde fue clasificada como maliciosa.



vemos que es maliciosa así encontrando la respuesta

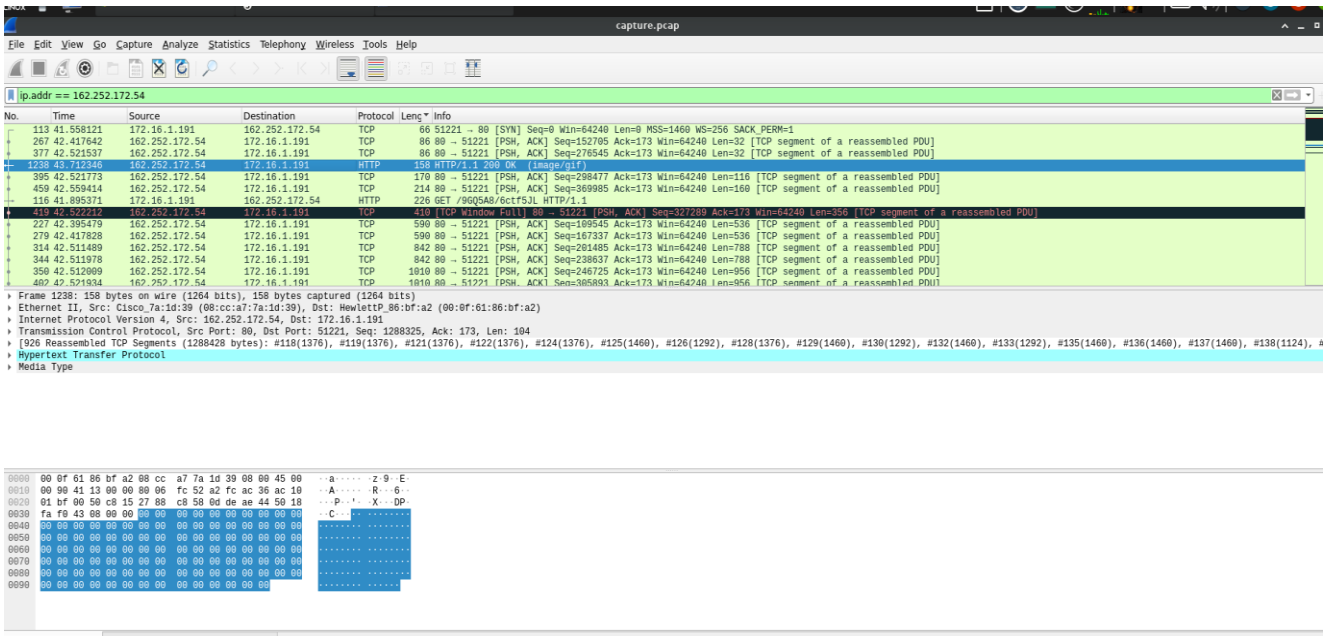


La flag: 162.252.172.54

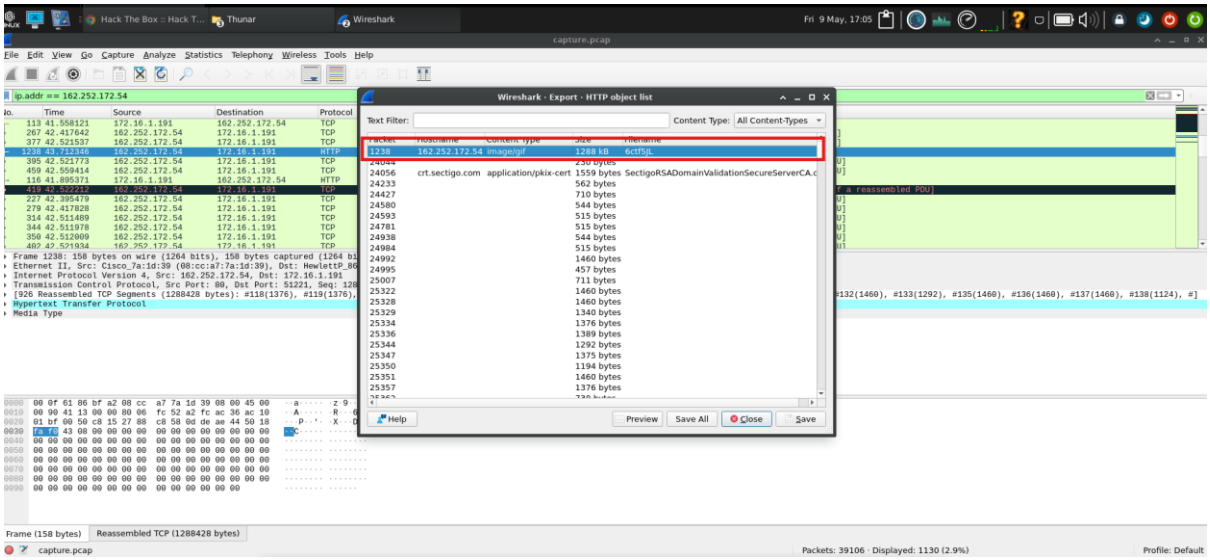
FLAG-2 Hash SHA-256 del archivo malicioso

Para identificar el hash 256 del malware me puse a observar las transferencia de dato de la ip atacante simplemente con el comando

ip.addr == 162.252.172.54

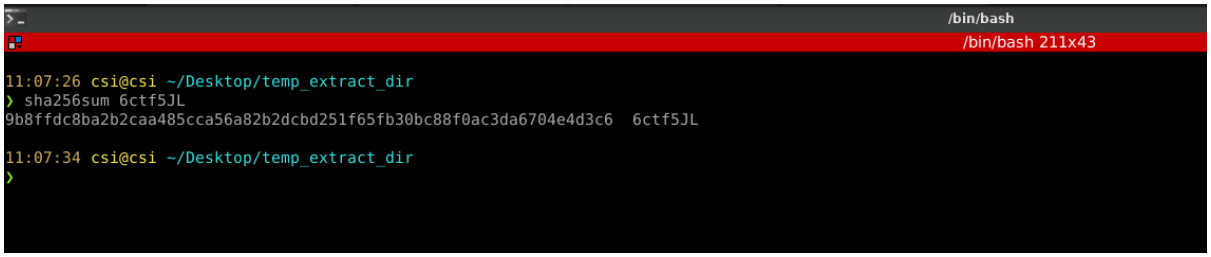


Esta transferencia de imagen exitosa de parte de la ip atacante comprueba un claro indicador del delivery del malware por lo que extraje esta imagen con el fin de comprobar el hash

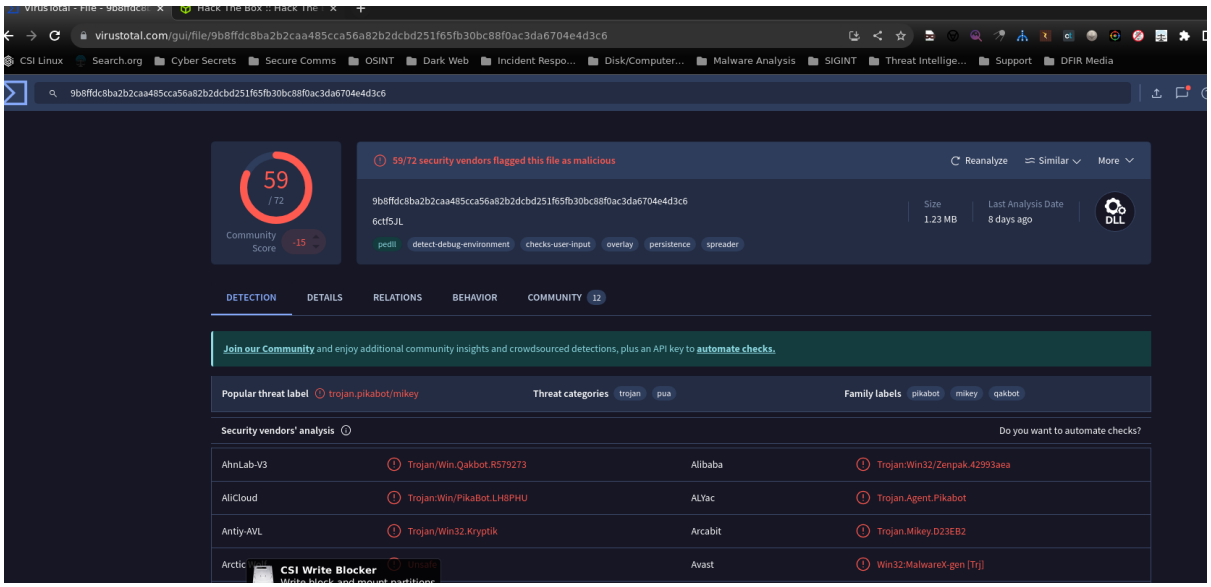


Luego procedí hacer la comprobación de hash con el comando

Sha256sum 6ctf5jl

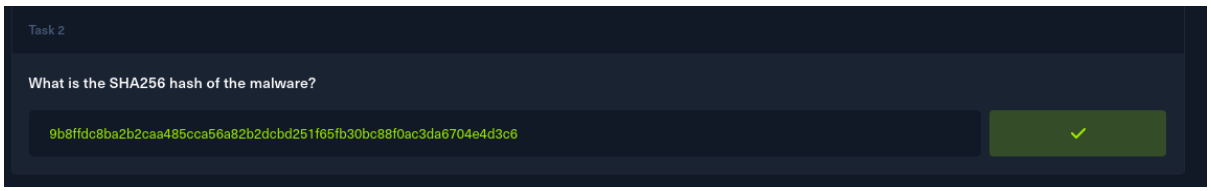


Procedi a llevar el hash a virus total a ver la reputación de este hash que presuntamente es del programa maligno



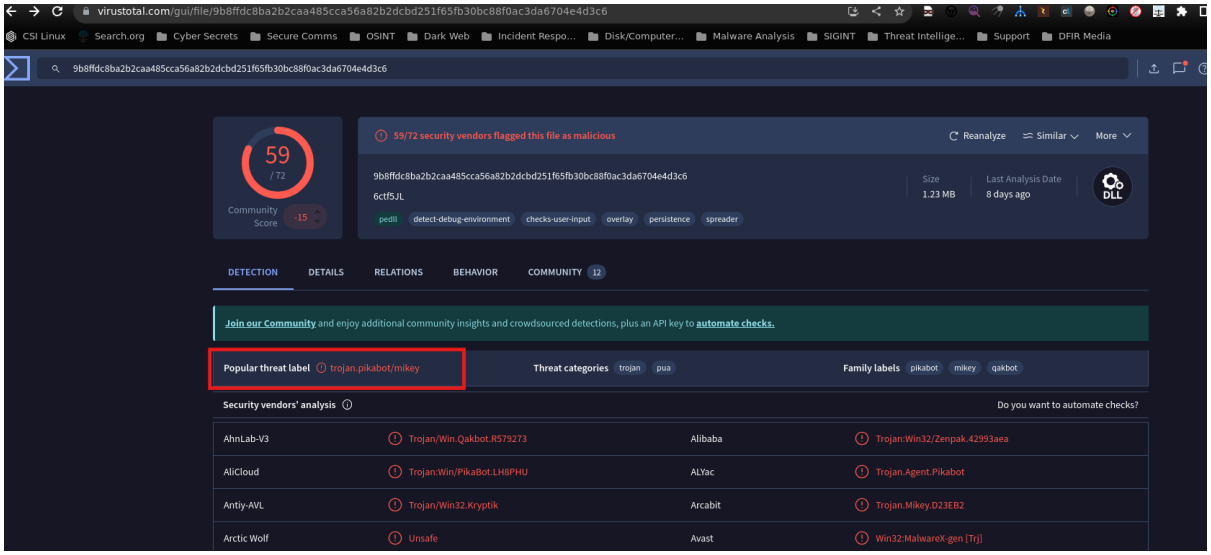
Asi encontrando la 2 flag:

9b8ffdc8ba2b2caa485cca56a82b2dcbd251f65fb30bc88f0ac3da6704e4d3c6



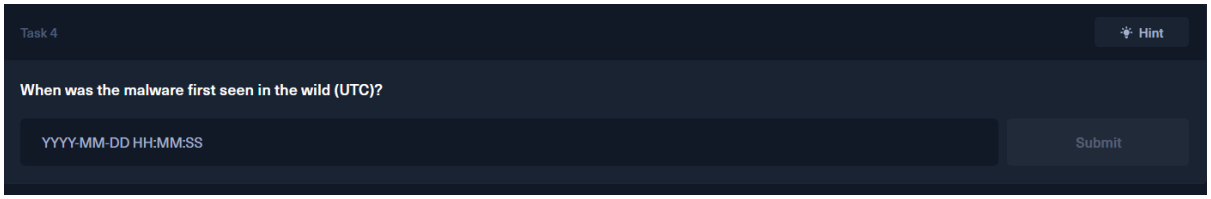
La Flag-3 Identificación de la familia del malware

Basándome en el análisis del hash proporcionado por Virus Total, pude identificar que el malware pertenece a la familia

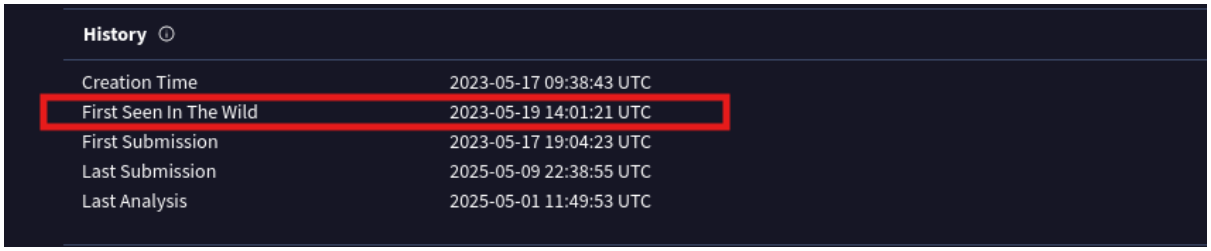


La FLAG: **pikabot**

La flag-4 Fecha de primera detección pública del malware

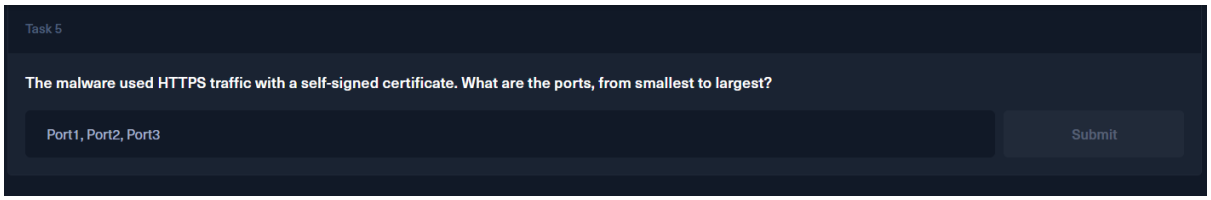


De igual manera nos vamos al apartado de detalles en virus total y encontramos la primera vez que se publicó el malware



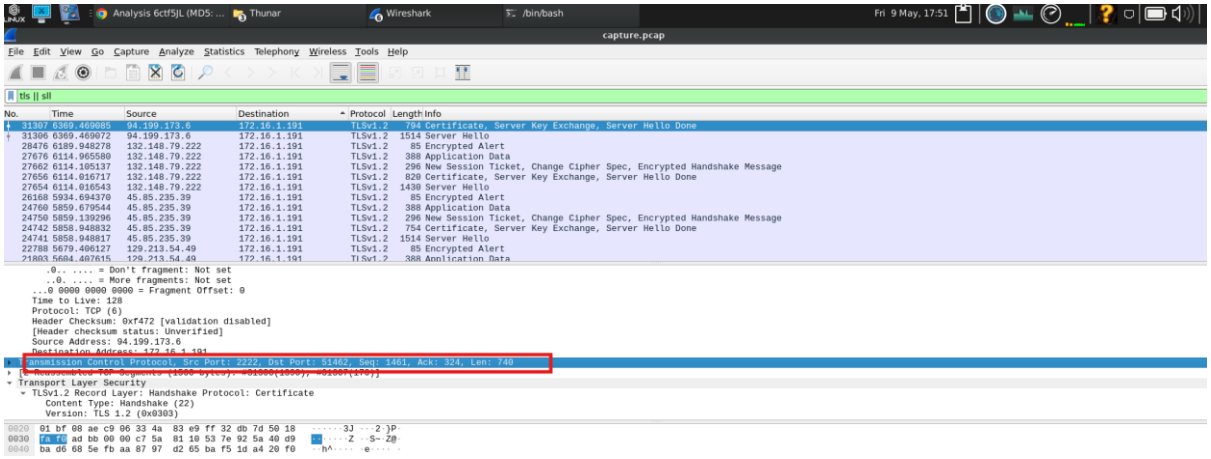
La flag: **2023-05-19 14:01:21**

Flag-5 Puertos utilizados por el atacante

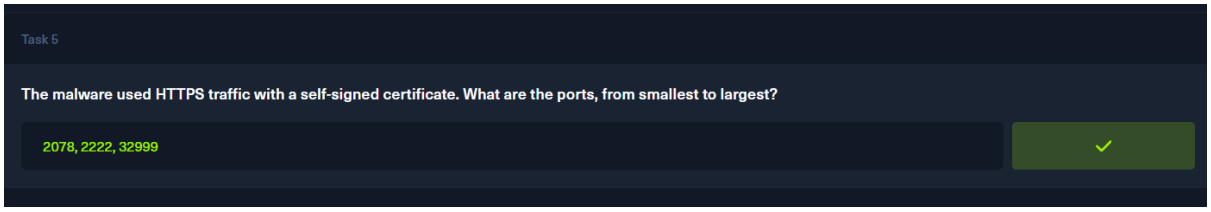


Para encontrar los puertos del trafico aplique el filtro tls || ssl

Asi encontrando los puertos de transferencia de control utilizada por el host

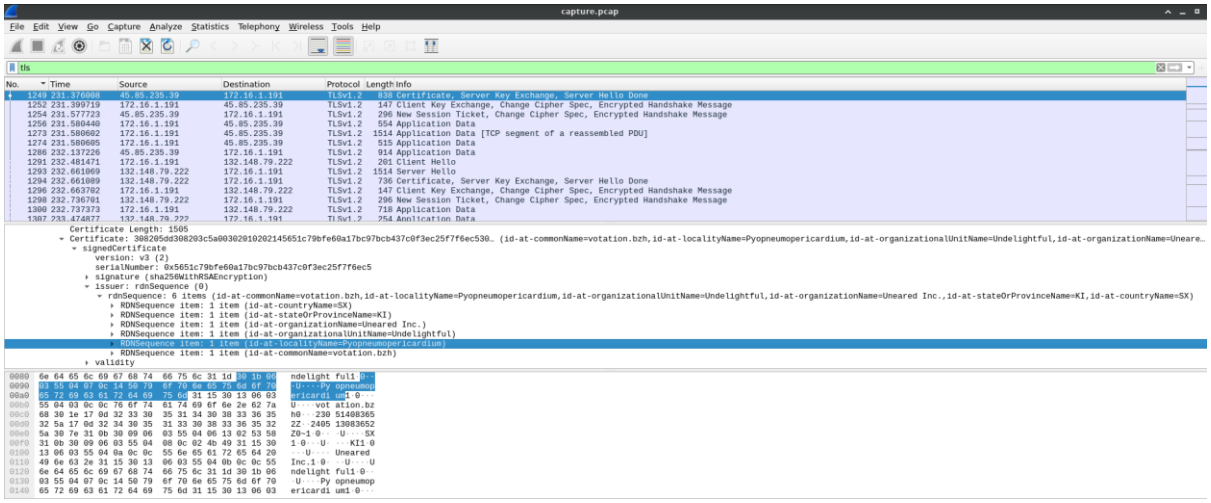


Encontrando 3 puerto en total son **2078, 2222, 32999**

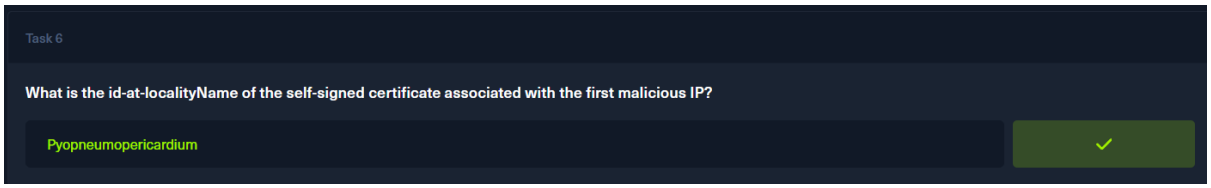


Flag-7 Campo inusual en el certificado TLS

Para encontrar esta seguí aplicando el filtro tls y entre al primer paquete que contiene información sobre certificado así encontrando la flag



La flag: **Pyopneumopericardium**

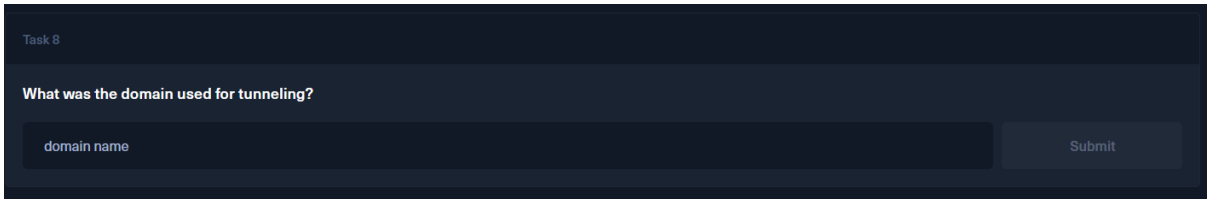


Flag-8 Hora UTC del certificado TLS

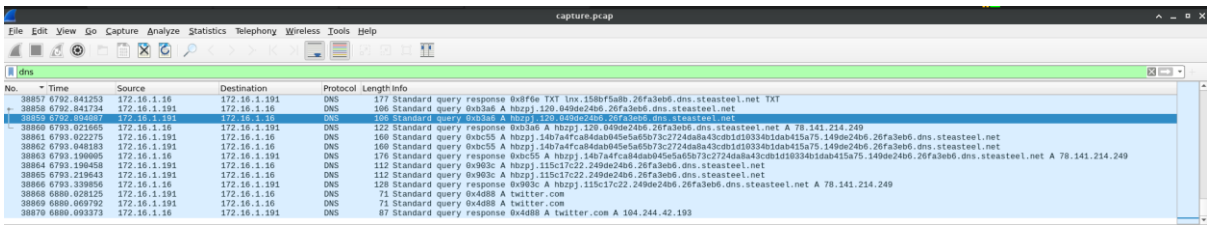
En el mismo paquete TLS que contenía el campo anterior, encontré también el timestamp UTC relacionado al certificado

La flag**: 2023-05-14 08:36:52**

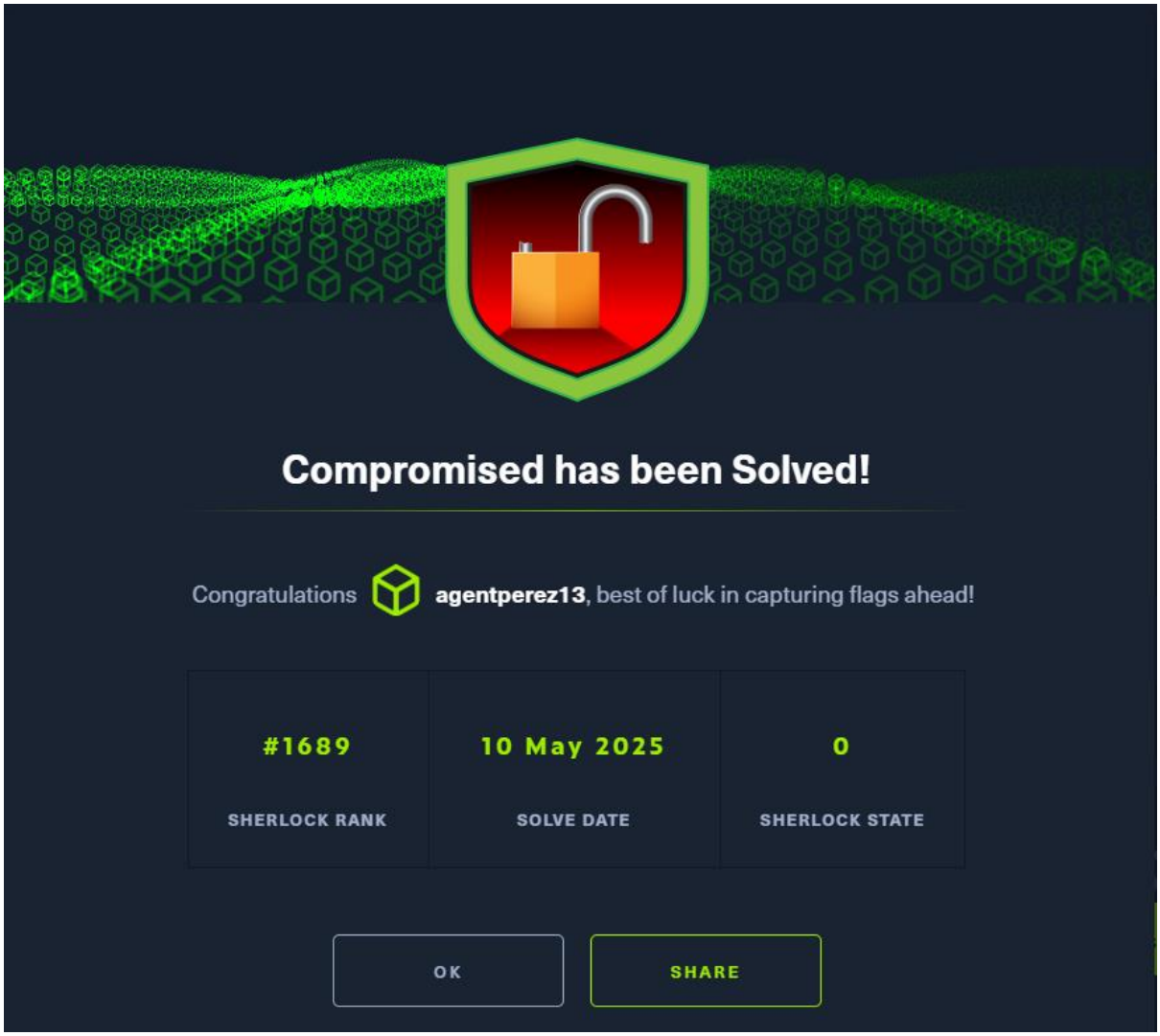
FLAG-9 – Dominio identificado



Utilizando un filtro DNS en Wireshark, accedí a las peticiones realizadas desde el host comprometido. Esto reveló un dominio utilizado por el atacante



La flag: steasteel.net



By Manuel Perez

NK Maloweer