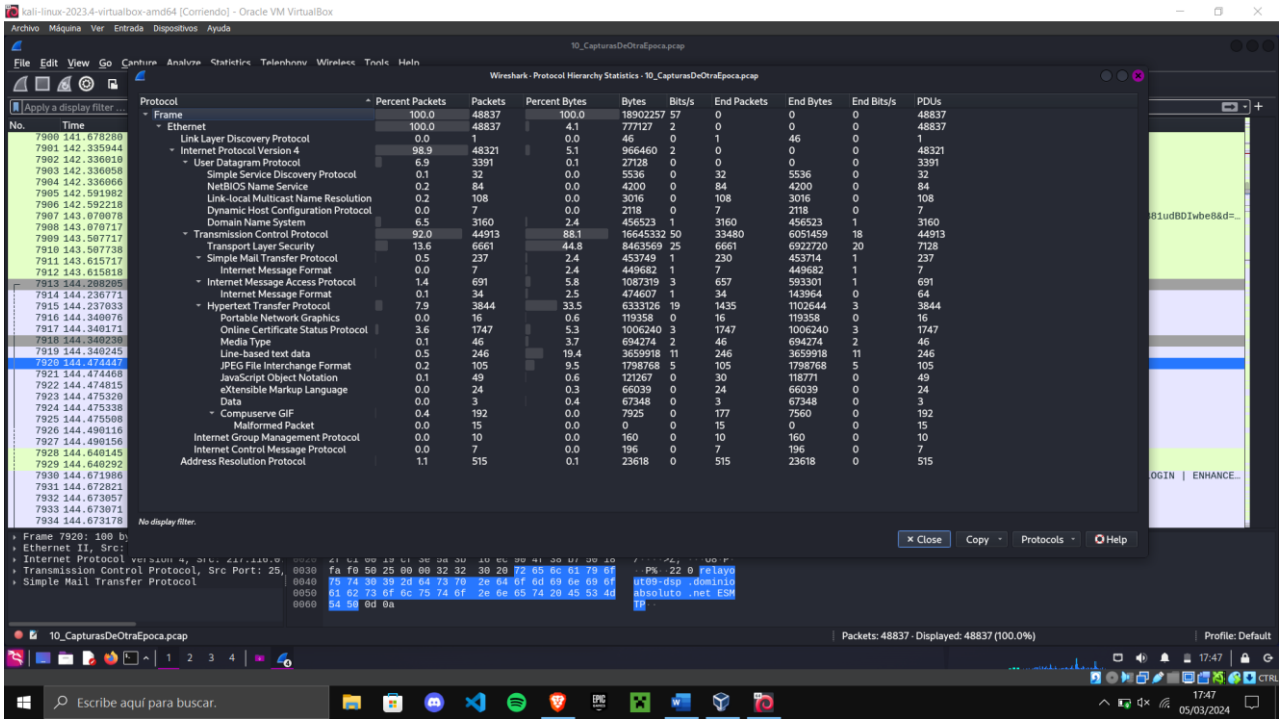
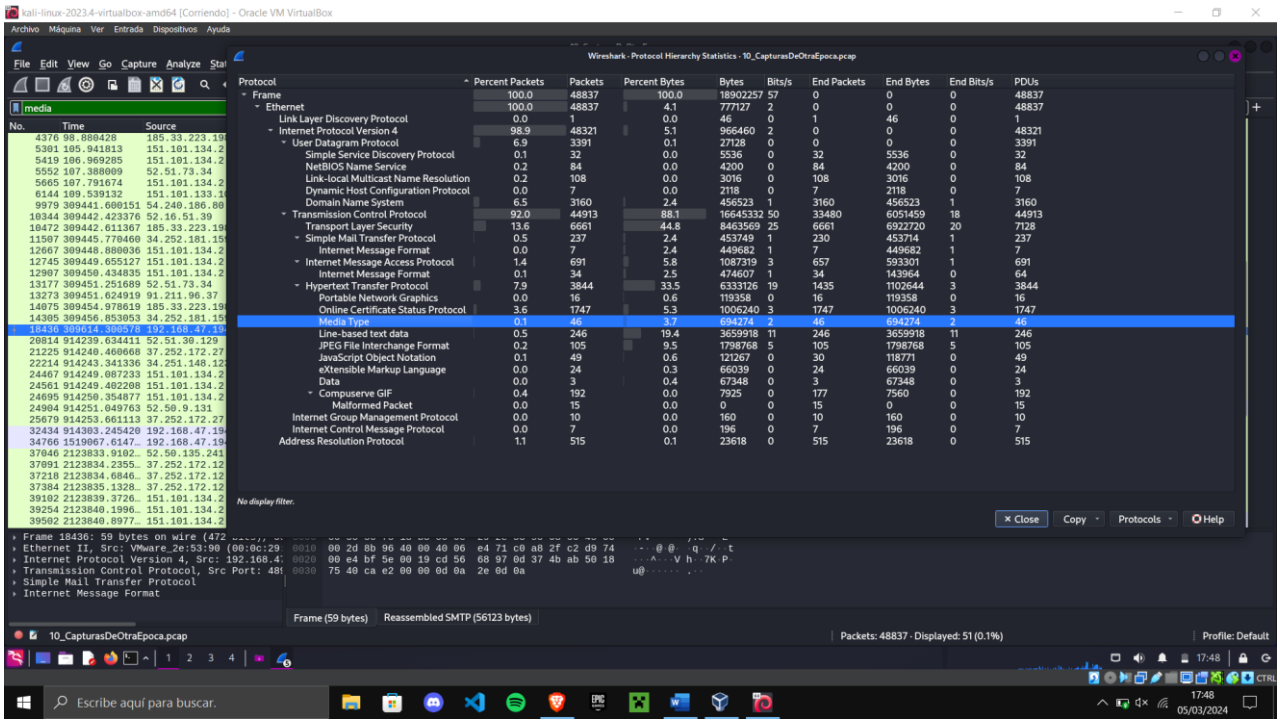
CAPTURAS DE OTRA ÉPOCA

Se ha detenido un sospechoso de ser infiltrado de una gran empresa en España que ha estado enviando un código a un asociado para informar sobre ciertas acciones previamente establecidas. Se necesita encontrar indicios de la supuesta clave que ha enviado. Se ha obtenido una captura de tráfico de su ordenador. Analízala para ver si existe algún tipo de mensaje o palabra clave que haya intentado ocultar con especial cuidado.

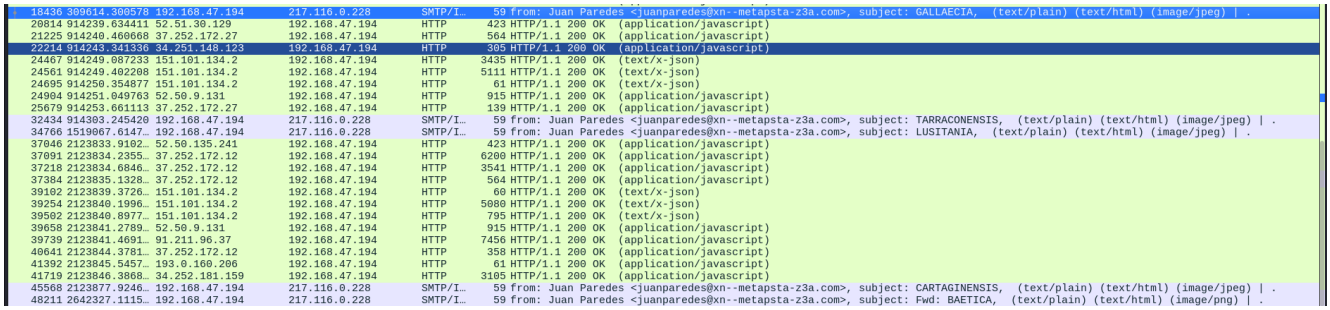
En primer lugar, hemos analizado el archivo .pcap proporcionado usando Wireshark:



Siguiendo Media Type nos encontramos lo siguiente:

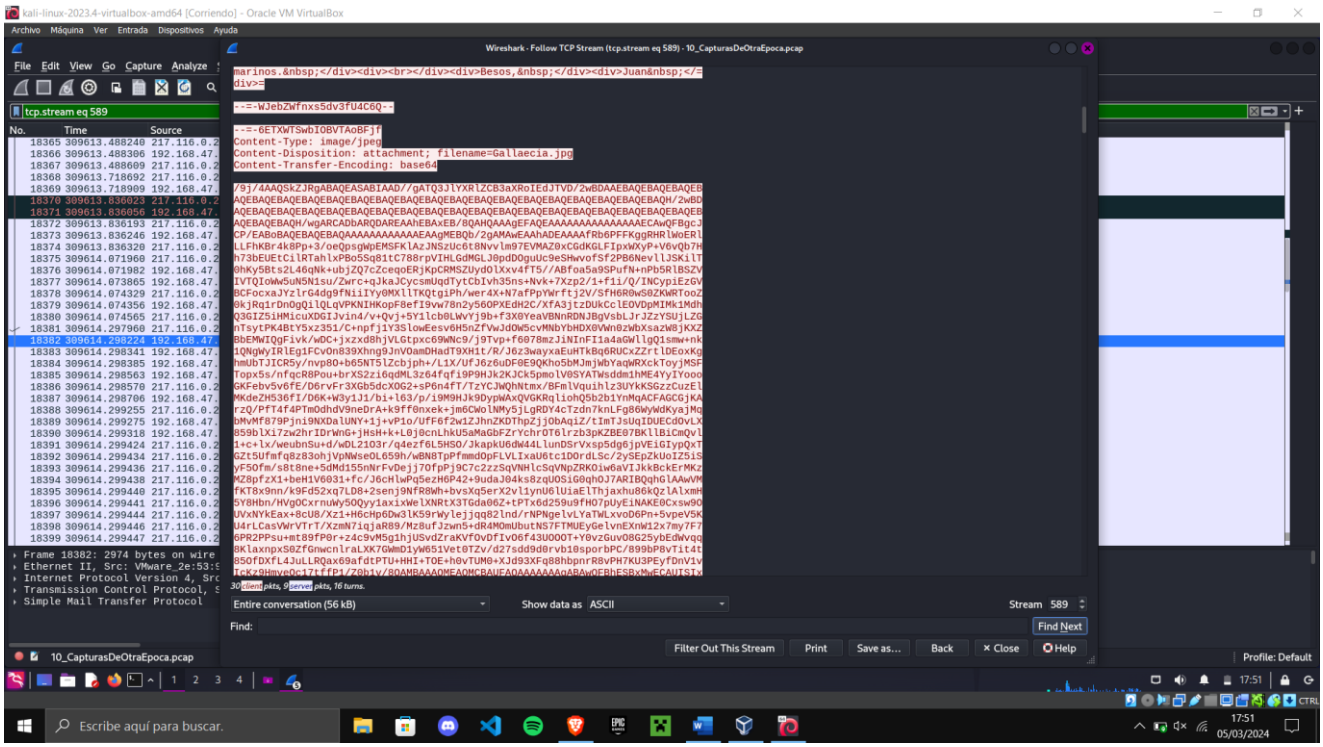


Donde podemos observar los correos:

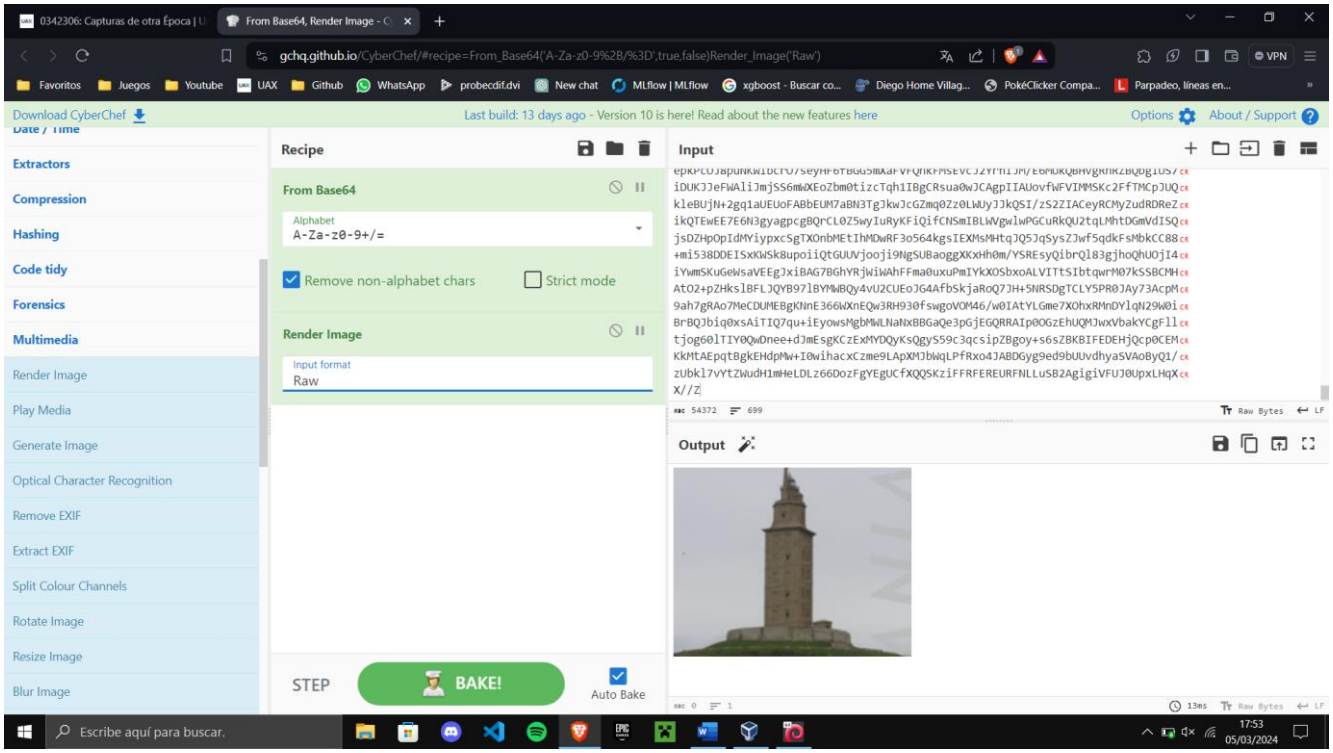


Y vemos que se están compartiendo archivos en formato .png y .jpeg.

Entrando en esos mensajes podemos encontrar la imagen codificada:



Descodificándola:



Y repitiendo esa operación acabamos obteniendo 5 imágenes:

Que superpuestas según la localización indicada por el nombre de la imagen resulta en un texto grisáceo:

Que resaltado saca el mensaje oculto HISPANIA:


HISPANIA