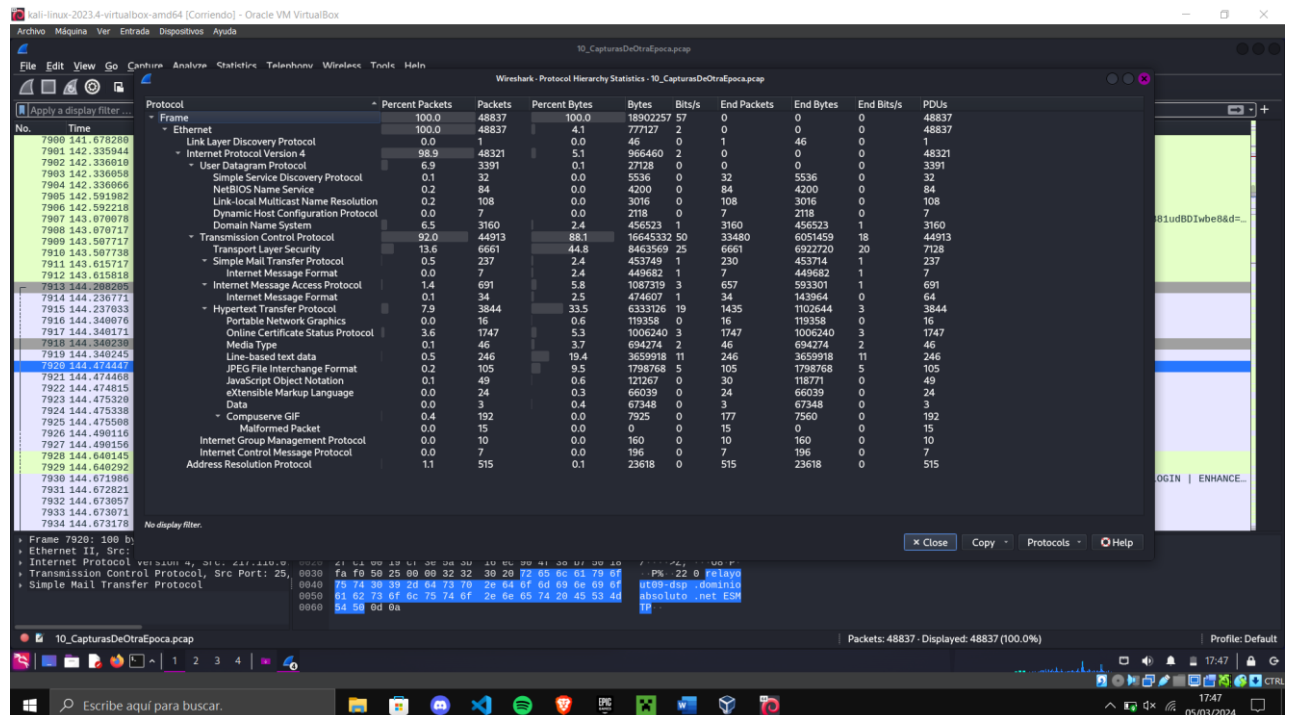


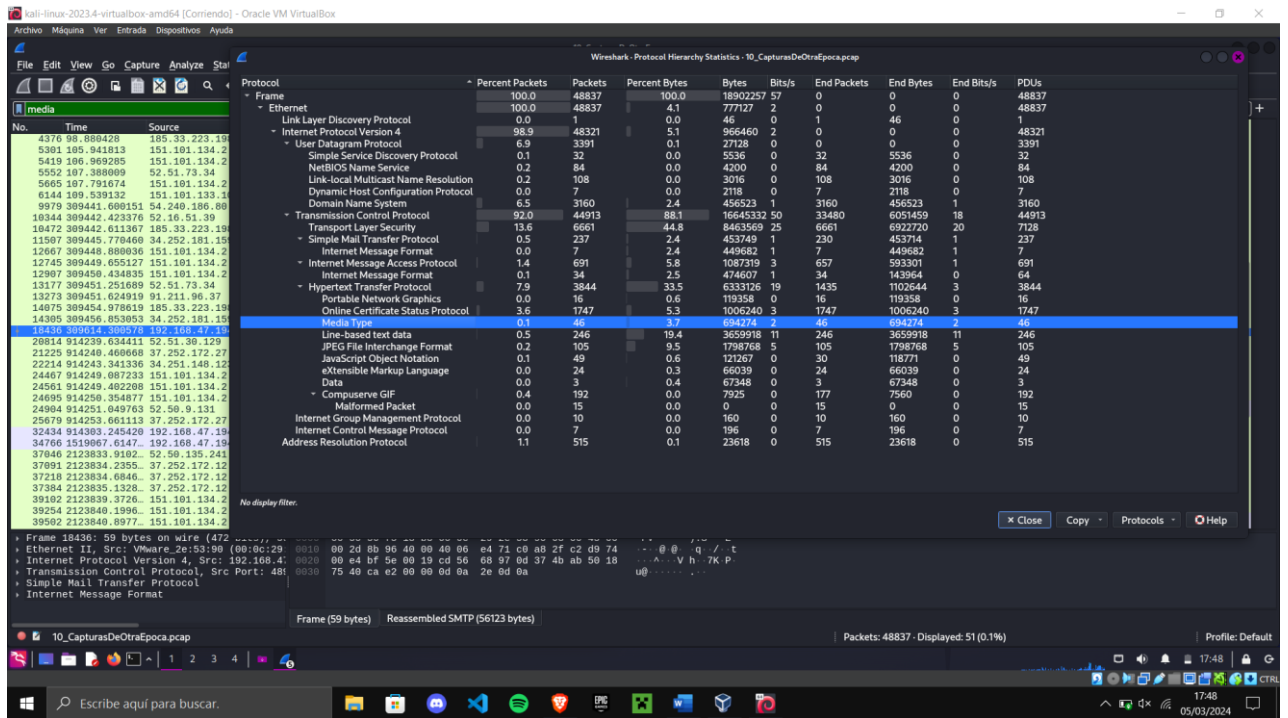
CAPTURAS DE OTRA ÉPOCA

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:



Seguindo Media Type nos encontramos lo siguiente:

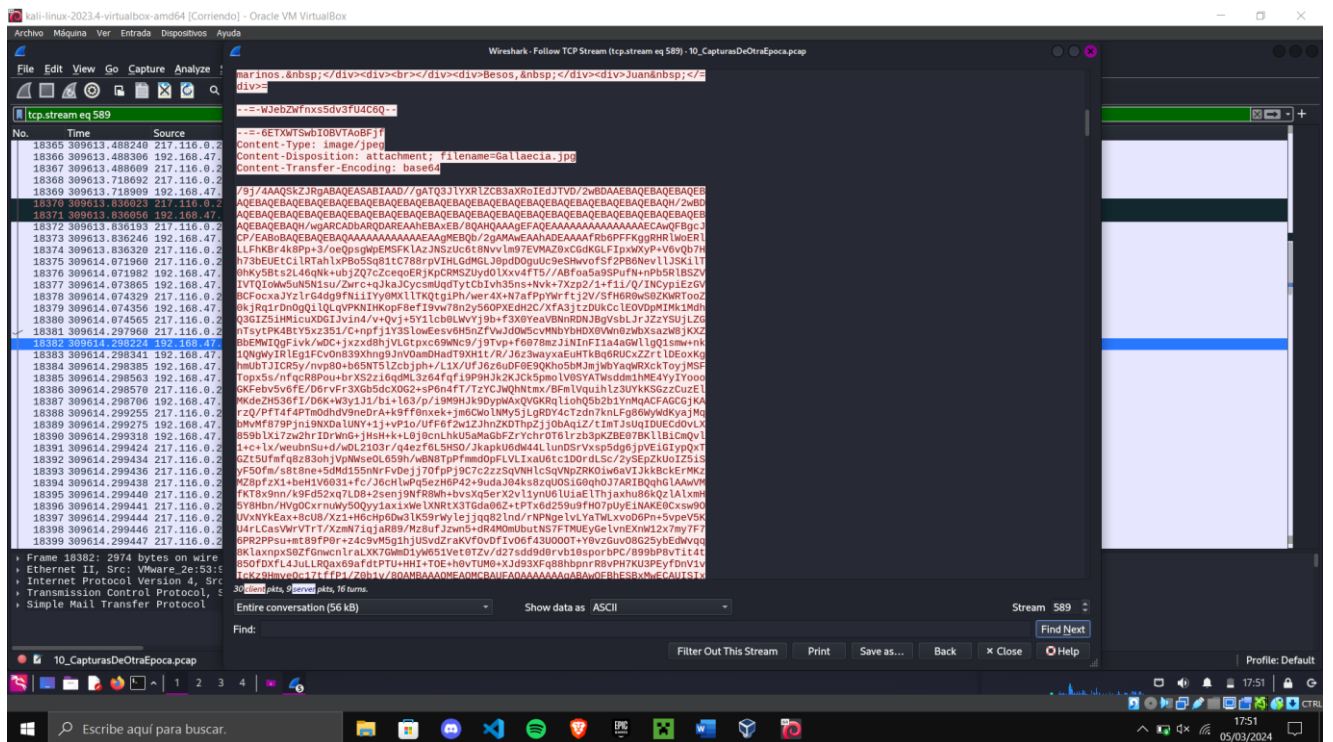


Donde podemos observar los correos:

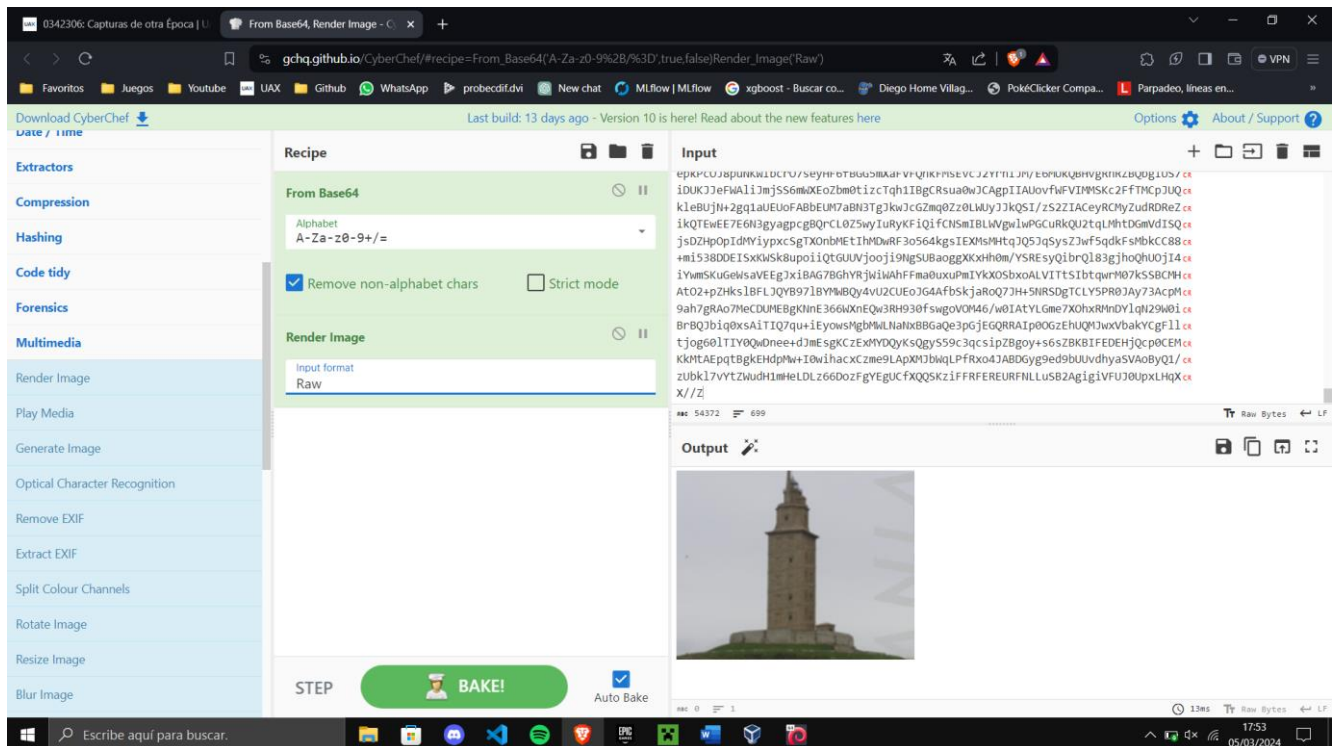
18436	389614.380578	192.168.47.194	217.116.0.228	SMTP/I..	59 from: Juan Paredes <juanparedes@xn--metapsta-z3a.com>, subject: GALLAECIA, (text/plain) (text/html) (image/jpeg) .
20814	914239.634411	52.51.30.129	192.168.47.194	HTTP	423 HTTP/1.1 200 OK (application/javascript)
21225	914240.460608	37.252.172.27	192.168.47.194	HTTP	564 HTTP/1.1 200 OK (application/javascript)
22214	914243.341336	34.251.148.12	192.168.47.194	HTTP	305 HTTP/1.1 200 OK (application/javascript)
24467	914249.087233	151.101.134.2	192.168.47.194	HTTP	3435 HTTP/1.1 200 OK (text/x-json)
24561	914249.402208	151.101.134.2	192.168.47.194	HTTP	5111 HTTP/1.1 200 OK (text/x-json)
24695	914250.354877	151.101.134.2	192.168.47.194	HTTP	61 HTTP/1.1 200 OK (text/x-json)
24894	914251.849763	52.50.9.131	192.168.47.194	HTTP	915 HTTP/1.1 200 OK (application/javascript)
25679	914253.661113	37.252.172.27	192.168.47.194	HTTP	139 HTTP/1.1 200 OK (application/javascript)
32434	914303.245420	192.168.47.194	217.116.0.228	SMTP/I..	59 from: Juan Paredes <juanparedes@xn--metapsta-z3a.com>, subject: TARRACONENSIS, (text/plain) (text/html) (image/jpeg) .
34766	1519067.6147..	192.168.47.194	217.116.0.228	SMTP/I..	59 from: Juan Paredes <juanparedes@xn--metapsta-z3a.com>, subject: LUSITANIA, (text/plain) (text/html) (image/jpeg) .
37846	2123833.9182..	52.50.135.241	192.168.47.194	HTTP	423 HTTP/1.1 200 OK (application/javascript)
37891	2123834.2355..	37.252.172.12	192.168.47.194	HTTP	6200 HTTP/1.1 200 OK (application/javascript)
37218	2123834.0846..	37.252.172.12	192.168.47.194	HTTP	3541 HTTP/1.1 200 OK (application/javascript)
37384	2123835.1328..	37.252.172.12	192.168.47.194	HTTP	564 HTTP/1.1 200 OK (application/javascript)
39182	2123839.3726..	151.101.134.2	192.168.47.194	HTTP	68 HTTP/1.1 200 OK (text/x-json)
39254	2123840.1996..	151.101.134.2	192.168.47.194	HTTP	5080 HTTP/1.1 200 OK (text/x-json)
39502	2123840.8977..	151.101.134.2	192.168.47.194	HTTP	795 HTTP/1.1 200 OK (text/x-json)
39658	2123841.2789..	52.50.9.131	192.168.47.194	HTTP	915 HTTP/1.1 200 OK (application/javascript)
39739	2123841.4691..	91.211.96.37	192.168.47.194	HTTP	7456 HTTP/1.1 200 OK (application/javascript)
40641	2123844.3781..	37.252.172.12	192.168.47.194	HTTP	358 HTTP/1.1 200 OK (application/javascript)
41392	2123845.5457..	193.0.160.200	192.168.47.194	HTTP	61 HTTP/1.1 200 OK (application/javascript)
41719	2123846.3098..	34.252.181.159	192.168.47.194	HTTP	3195 HTTP/1.1 200 OK (application/javascript)
45508	2123877.9246..	192.168.47.194	217.116.0.228	SMTP/I..	59 from: Juan Paredes <juanparedes@xn--metapsta-z3a.com>, subject: CARTAGINENSIS, (text/plain) (text/html) (image/jpeg) .
48211	2642327.1115..	192.168.47.194	217.116.0.228	SMTP/I..	59 from: Juan Paredes <juanparedes@xn--metapsta-z3a.com>, subject: Fwd: BAETICA, (text/plain) (text/html) (image/png) .

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