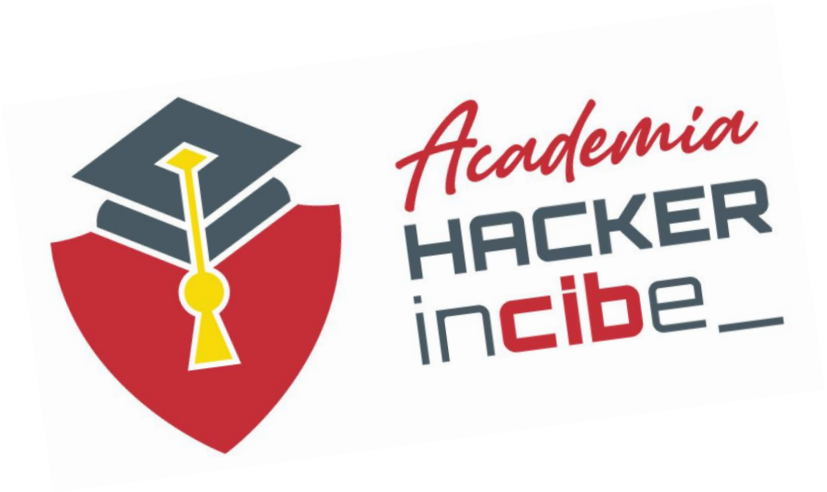
GOBIERNO DE ESPAÑA
VICEPRESIDENCIA PRIMERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL



Academia Hacker INCIBE

Capturas de otra época

Dificultad: **Media**

Categoría de Reto: **Forense**

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017 TU AYUDA EN CIBERSEGURIDAD

Contenido

ÍNDICE DE FIGURAS

No se encuentran elementos de tabla de ilustraciones.

ÍNDICE DE TABLAS

No se encuentran elementos de tabla de ilustraciones.

1. CONTEXTO

Identificar el código que un sospechoso infiltrado ha mandado dentro de una captura de tráfico de red.

Flag: **HISPANIA**

Datos Proporcionados:

- Archivo .pcap

2. DESCRIPCIÓN PARA PARTICIPANTES

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.

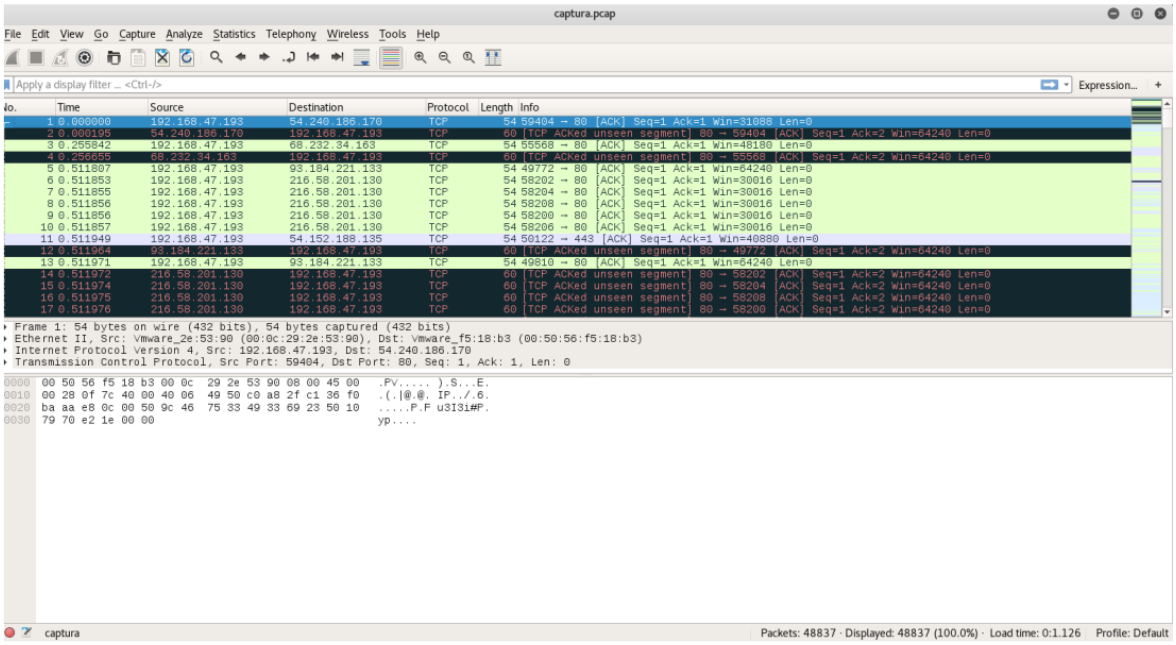
3. PISTAS

1. Examina la captura de tráfico con algún programa apropiado. La información que se transmite por correo electrónico puede ser de especial interés.
2. Los emails pueden tener archivos adjuntos.
3. Varias imágenes pueden formar una gran imagen.

4. SOLUCIÓN

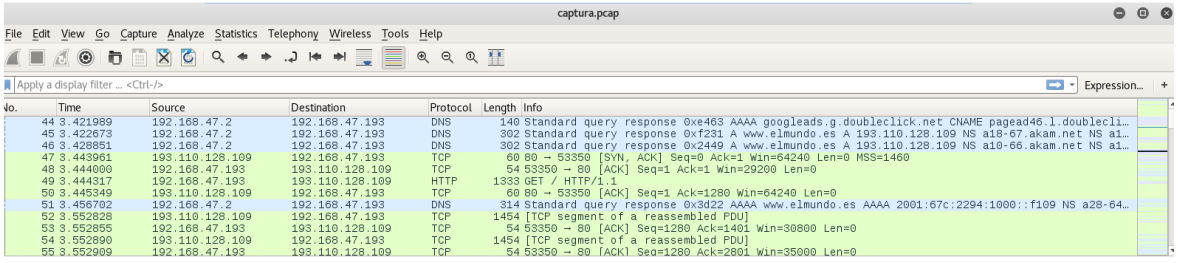
4.1. Opción 1

Descargamos y abrimos la captura pcap con un programa que nos permita leer el tráfico. Se utilizará Wireshark en nuestro caso.



Echamos un primer vistazo a la captura, pero al ser tan extensa, nos planteamos de qué formas habría podido el sospechoso mandar un código sin llamar la atención.

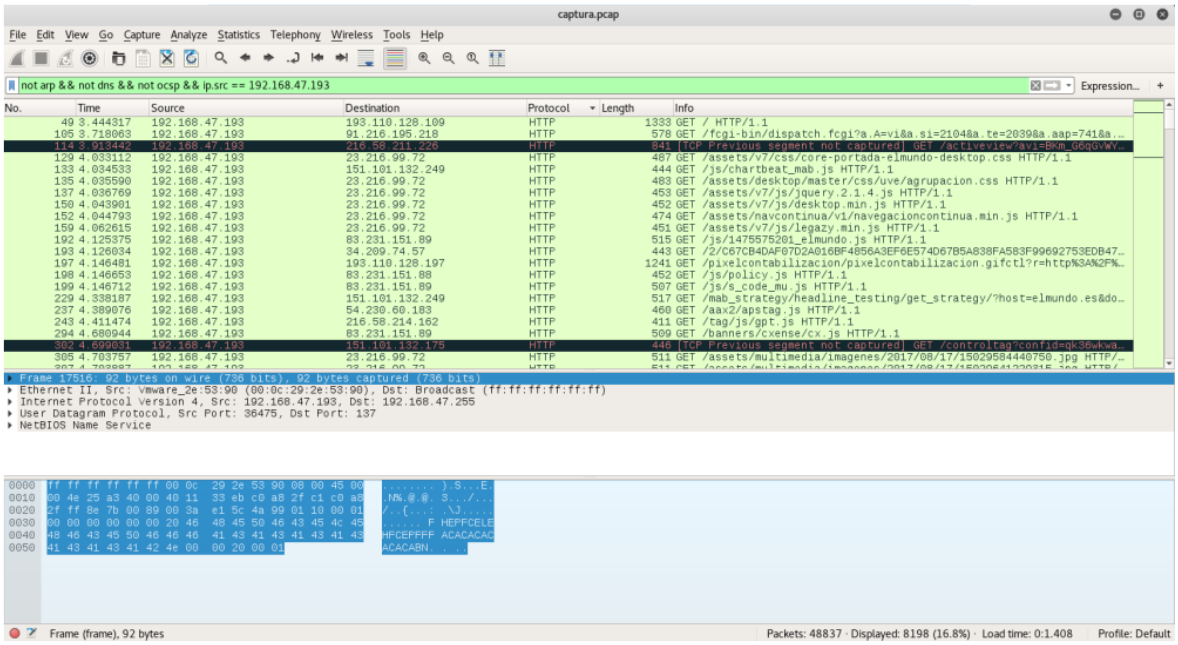
Vamos a identificar la IP del ordenador desde el que se realizan las conexiones salientes, que en este caso observamos por el intercambio de paquetes: 192.168.47.193, y se va a intentar filtrar protocolos que a priori lo único que hacen es meter ruido a la captura.



Realizamos el filtrado y después ordenamos los paquetes por protocolos:

```
not arp && not dns && not ocsp && ip.src == 192.168.47.193
```

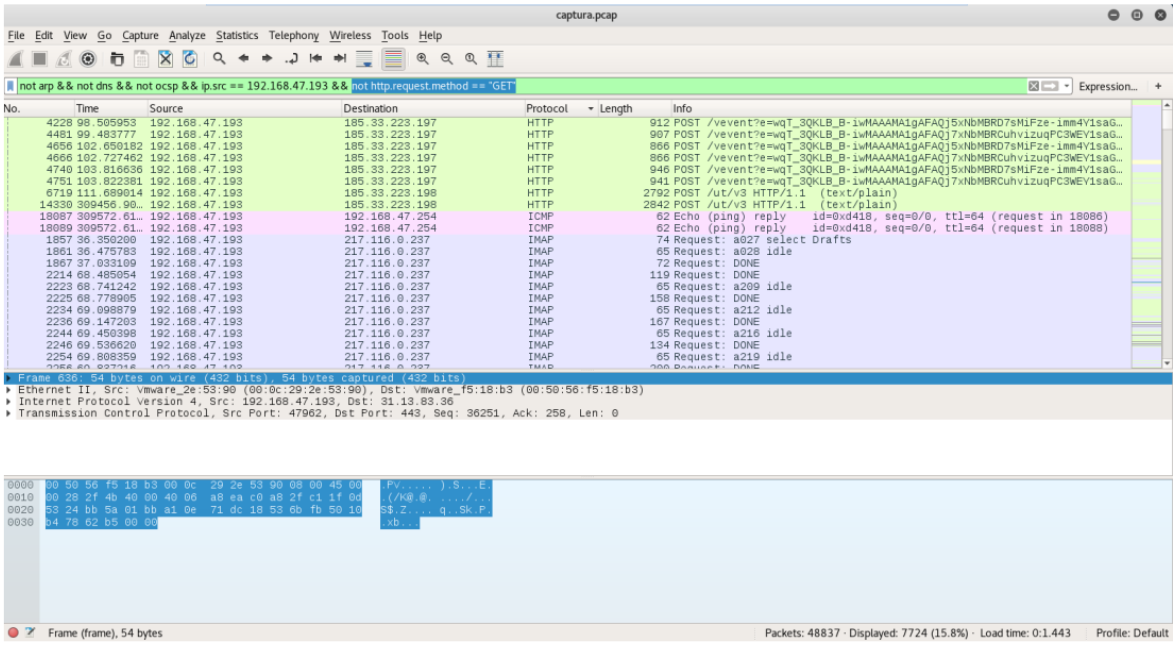
Tras ello, se ha conseguido reducir la captura a un 16,8%, lo cual nos permite echar otro vistazo más conciso sobre ella para ver si detectamos algo que nos pueda indicar cómo se ha podido comunicar el código:



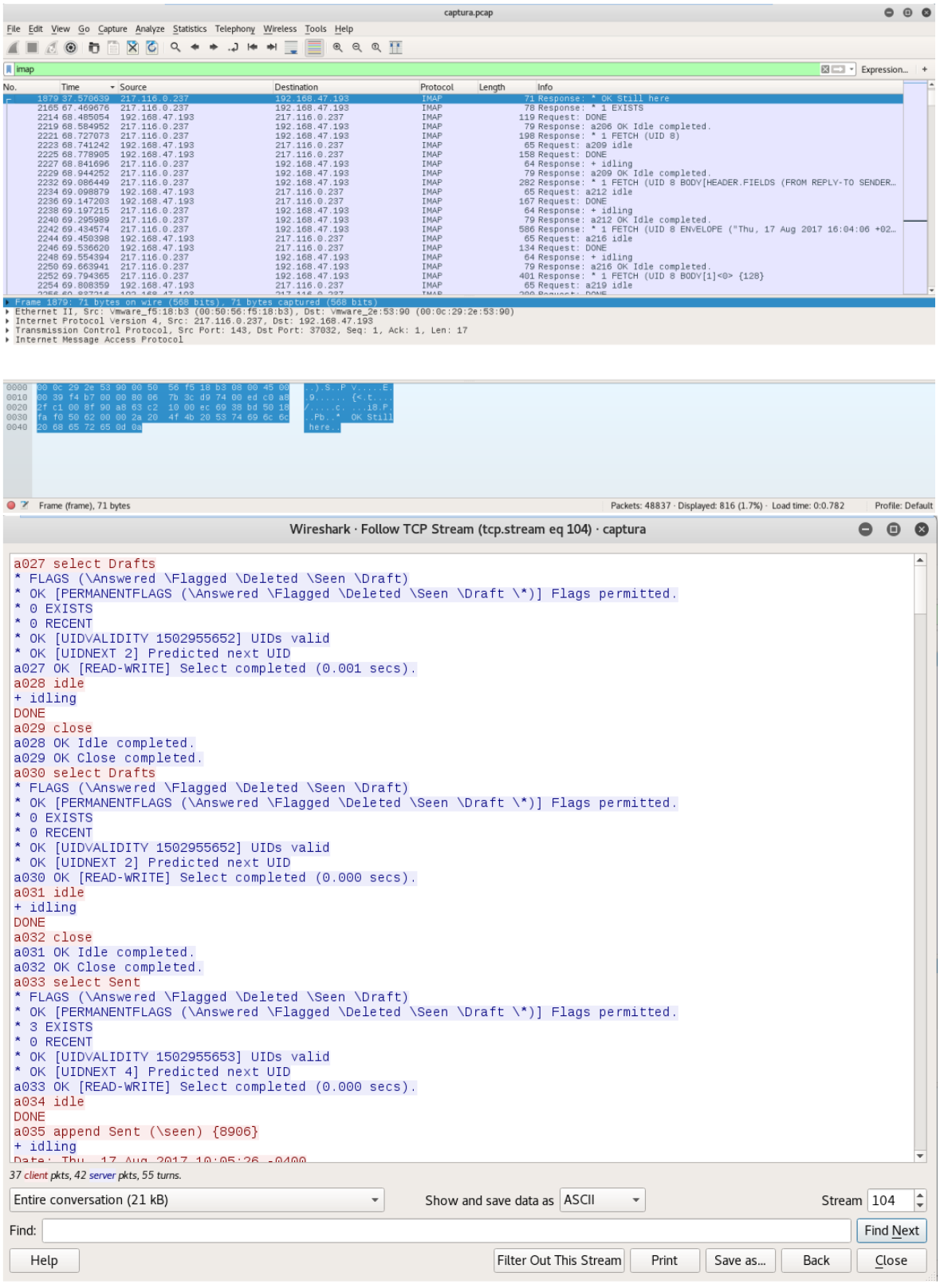
Y tras ver que existen peticiones GET por http, que parecen no aportar nada vamos a añadir otro filtro para eliminarlas:

not http.request.method == "GET"

Quedándose la captura así:

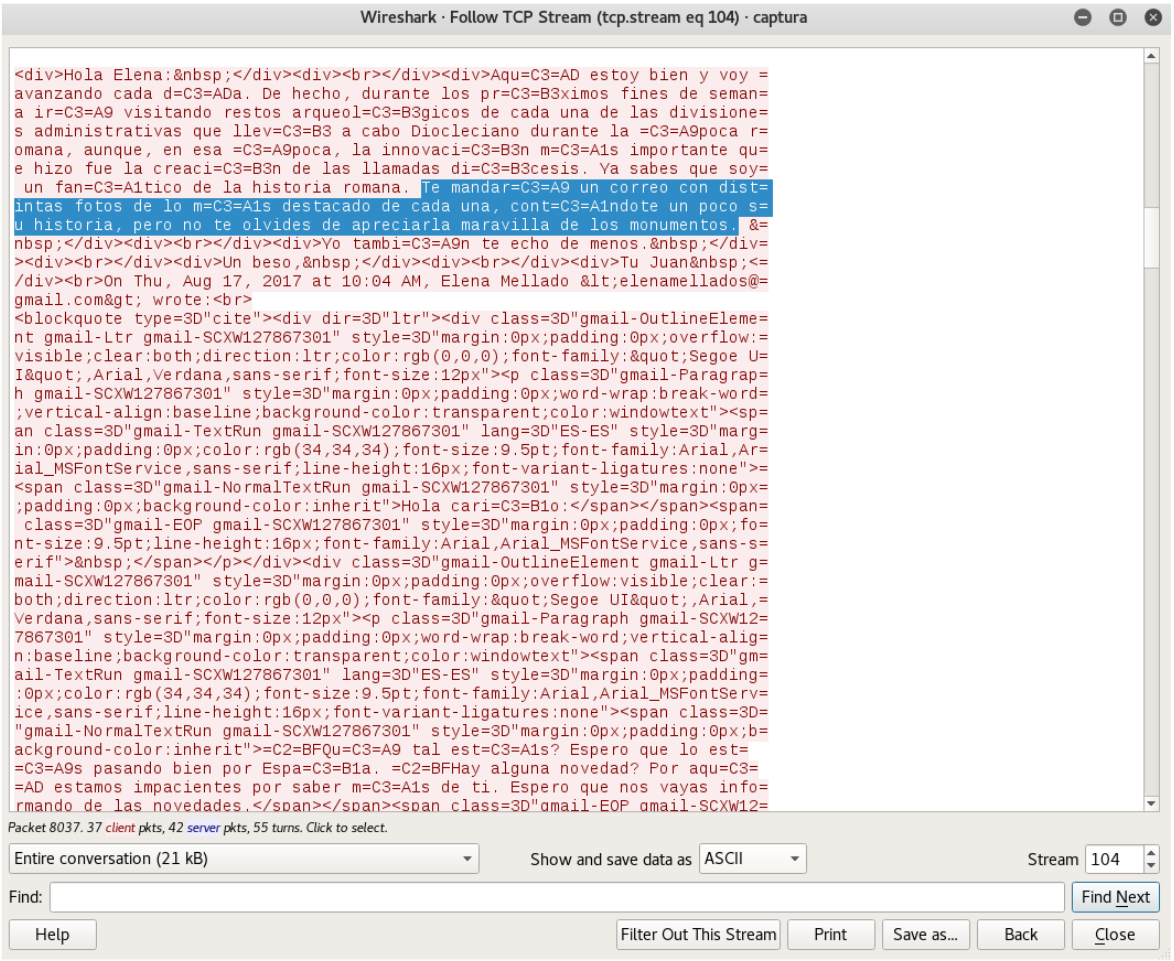


Bajando entre los paquetes vemos que tenemos paquetes IMAP correspondientes a un intercambio de correos electrónicos. Por lo que vamos a filtrar sólo ese protocolo, ordenar los paquetes por tiempo y hacer un Follow TCP Stream para observar más rápidamente la información intercambiada.



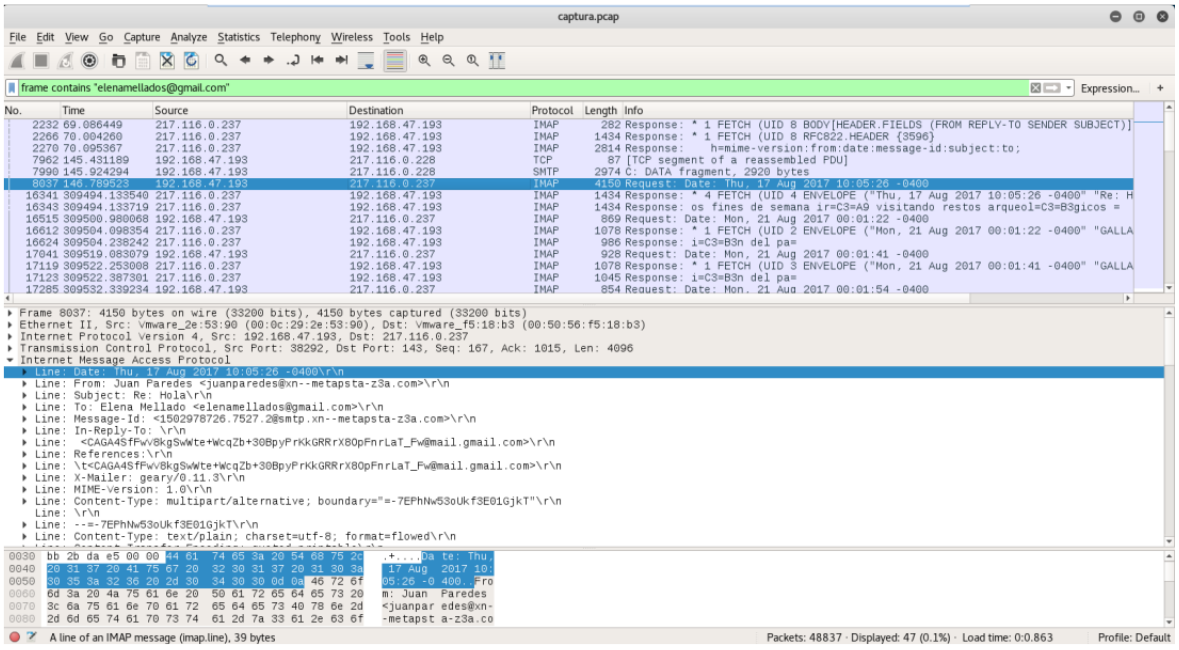
Si vamos observando la información que nos aporta el Follow TCP Stream, observamos que siempre ha habido un intercambio de mensajes entre nuestro sospechoso, mediante su cuenta juanparedes@xn--metapsta-z3a.com, y otra persona cuya cuenta es elenamellados@gmail.com.

En uno de los correos que le manda Juan a Elena dice que va a enviar varias fotografías en las próximas semanas, mientras visita varias zonas cada una correspondiente a las divisiones administrativas en España que se llevaron a cabo en la época de Diocleciano. Esas fotografías puede que nos puedan interesar por ello vamos a extraerlas de la captura. Además, Juan remarca la importancia de esas fotos.



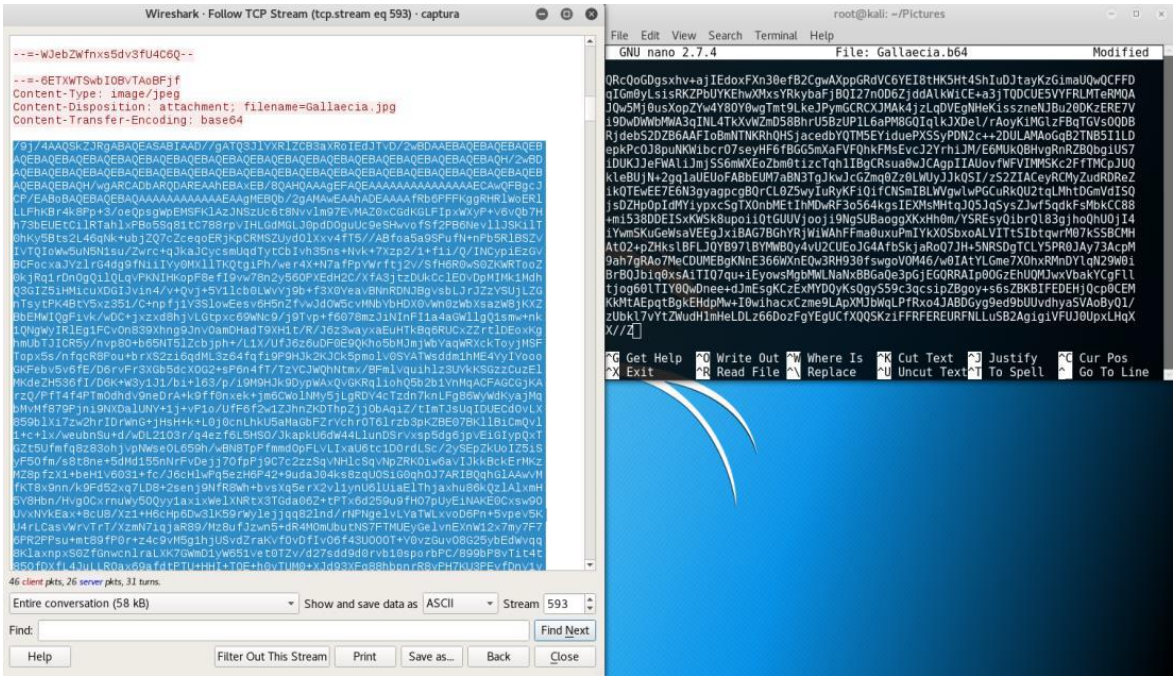
Ahora vamos a filtrar entre los paquetes que se dirijan a Elena:

frame contains elenamellados@gmail.com



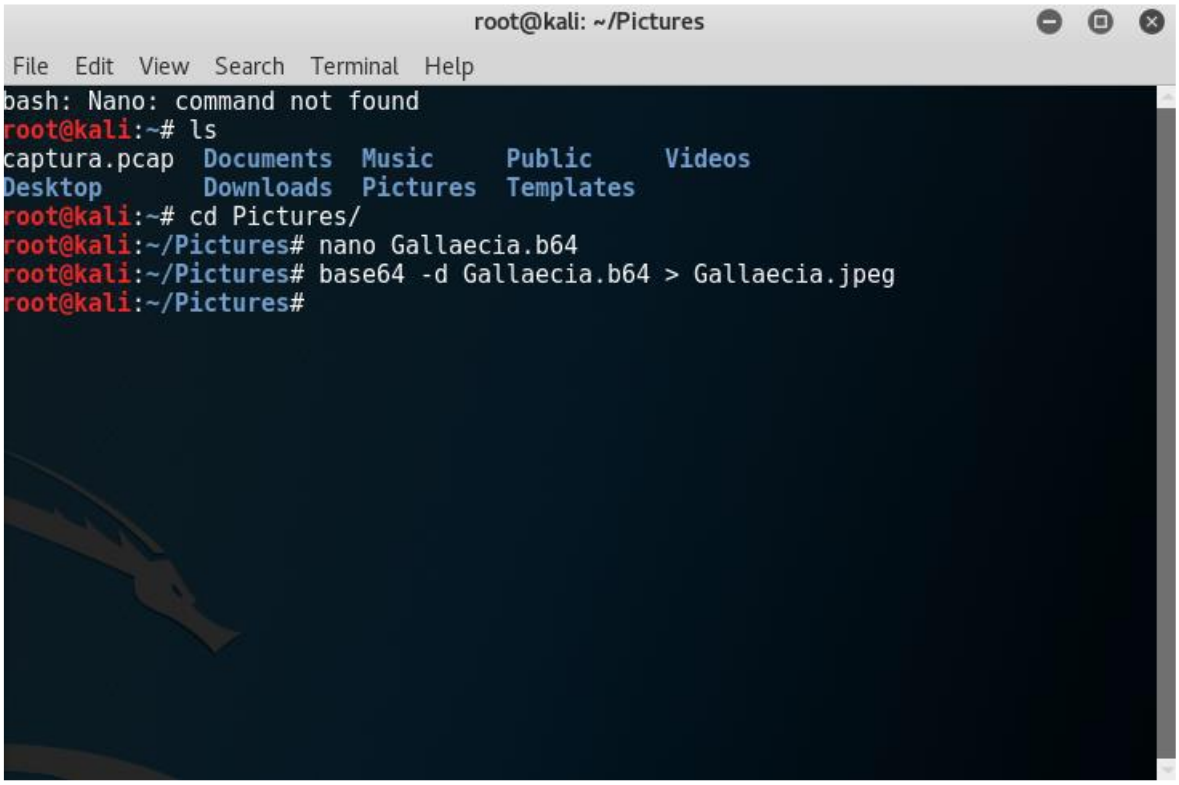
Y vamos a sacar esas fotos enviadas a Elena de cada uno de los paquetes. Para ello seguiremos siempre el siguiente procedimiento. Abrimos el primero de los correos referido en este caso a GALLAECIA, es decir, haremos un Flollow TCP Stream a ese paquete. Dentro del paquete vemos que viene una imagen adjunta en formato jpeg y codificada en base64.

A continuación, necesitamos decodificar de base64 a imagen. Para ello, copiamos la imagen en base64 en un nuevo fichero al que le pondremos la extensión .b64.



Y para sacar la imagen en consola metemos el siguiente comando:

base64 –d Gallaecia.bs64 > Gallaecia.jpeg

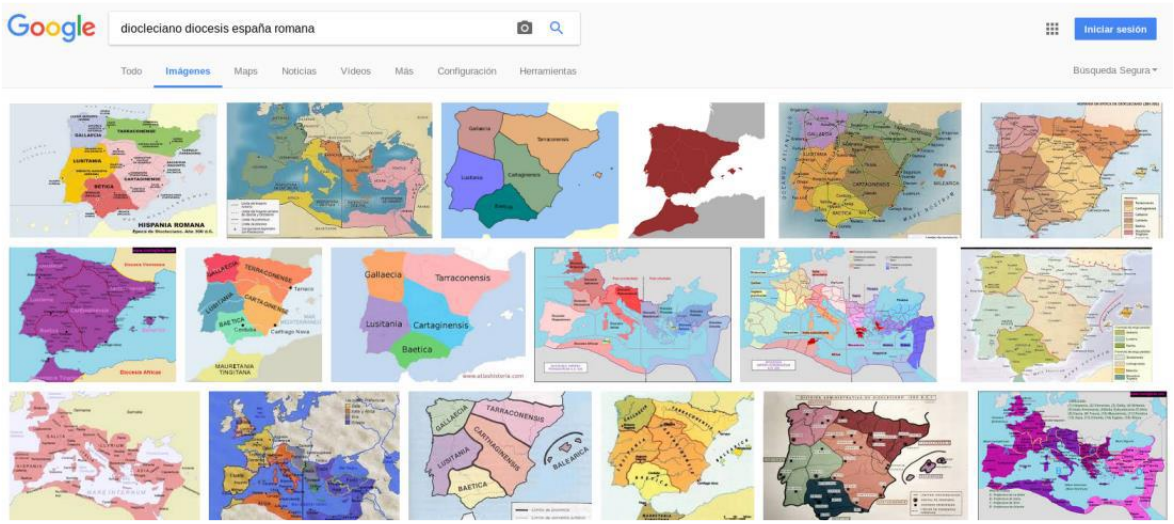


Y obtenemos nuestra imagen:

Repetimos la misma operación para cada una de las imágenes.

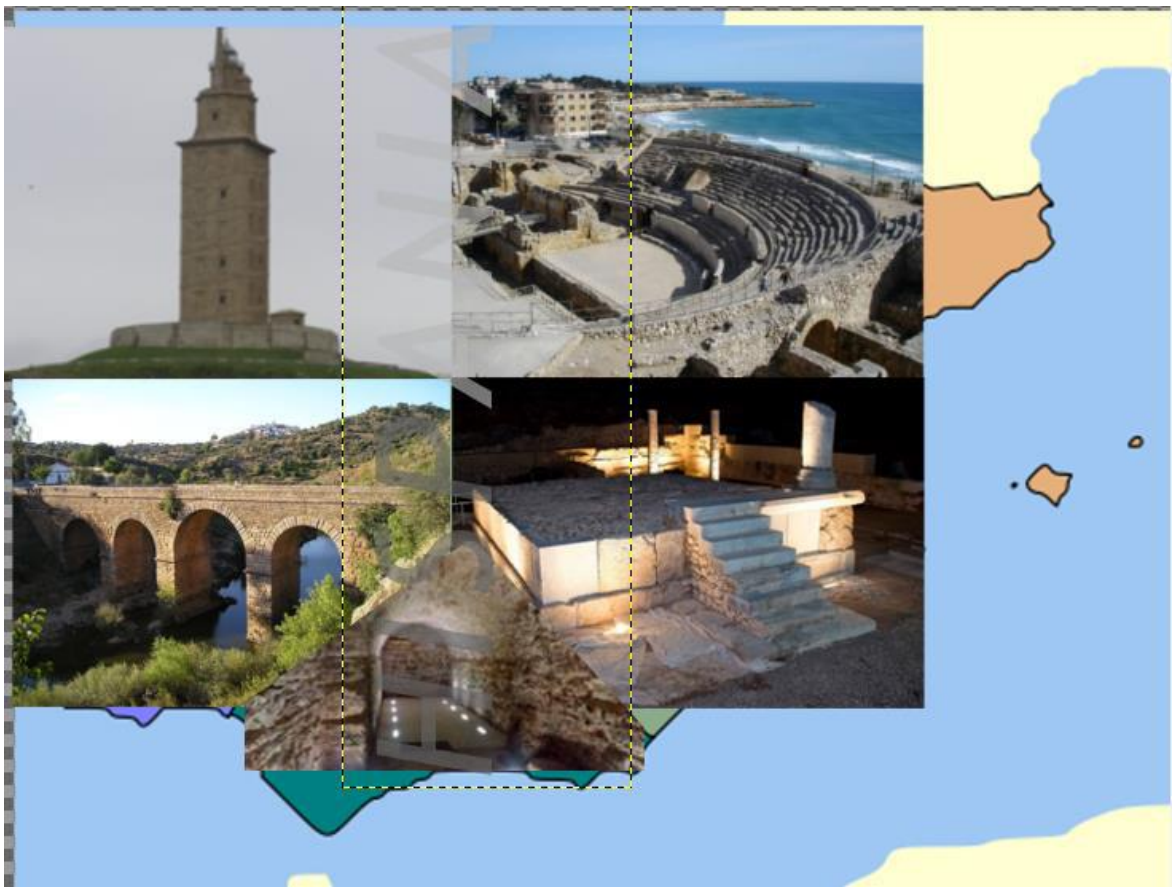
GALLAECIA, TARRACONENSIS, LUSITANIA, CARTAGINENSIS y BAETICA.

Una vez obtenidas todas las imágenes, recordamos que Juan hizo mención en su primer email a una distribución territorial de España por diócesis llevada a cabo por Diocleciano durante la época romana. Buscamos en internet cómo queda distribuida España según esa reforma.



En la tercera imagen de la búsqueda podemos ver claramente esa distribución, que es en la que nos vamos a basar para hacer la composición con las imágenes obtenidas.

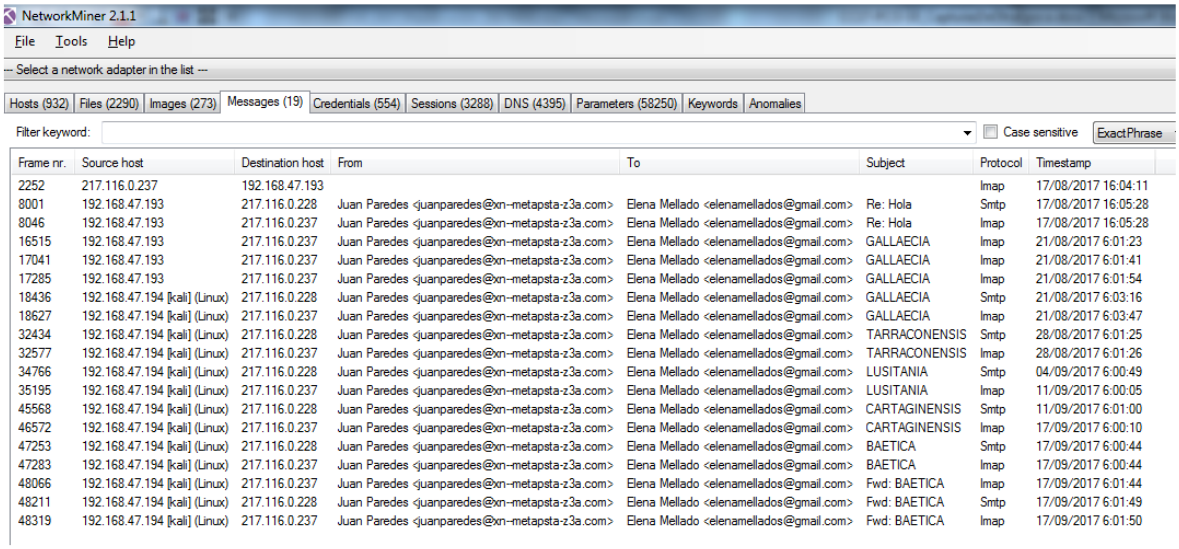
Para ello abrimos un editor fotográfico. En este caso, se ha usado Gimp y tras hacer la composición basada en el mapa nos queda algo así:



Tras ello, podemos descubrir el código que nos servirá como prueba final para inculpar al sospechoso y salvar nuestro país.

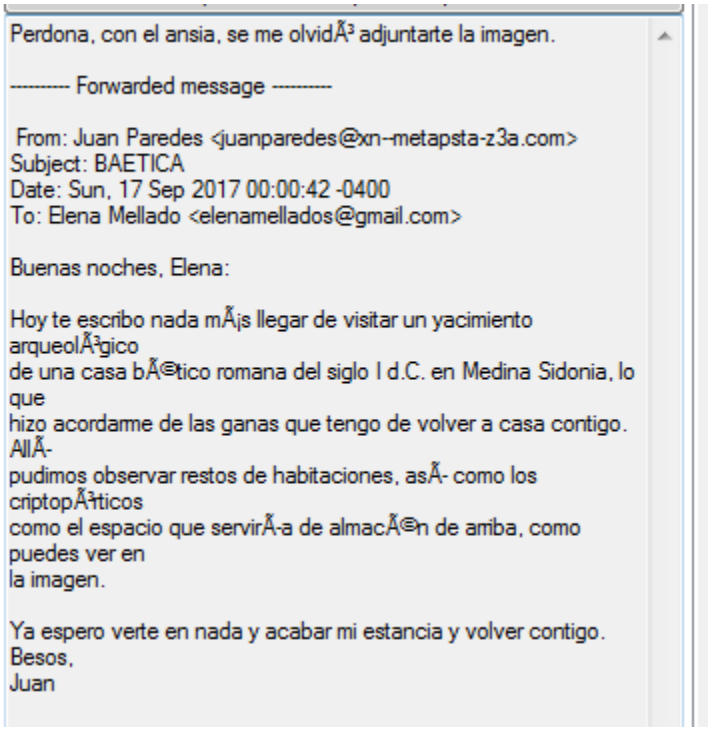
4.2. Opción 2

Utilizando otro software como NetworkMiner para extraer el contenido de la captura de tráfico se pueden obtener los correos electrónicos que se encuentran en la captura de tráfico:



Frame nr.	Source host	Destination host	From	To	Subject	Protocol	Timestamp
2252	217.116.0.237	192.168.47.193				Imap	17/08/2017 16:04:11
8001	192.168.47.193	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Re: Hola	Smtp	17/08/2017 16:05:28
8046	192.168.47.193	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Re: Hola	Imap	17/08/2017 16:05:28
16515	192.168.47.193	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Imap	21/08/2017 6:01:23
17041	192.168.47.193	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Imap	21/08/2017 6:01:41
17285	192.168.47.193	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Imap	21/08/2017 6:01:54
18436	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Smtp	21/08/2017 6:03:16
18627	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Imap	21/08/2017 6:03:47
32434	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	TARRACONENSIS	Smtp	28/08/2017 6:01:25
32577	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	TARRACONENSIS	Imap	28/08/2017 6:01:26
34766	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	LUSITANIA	Smtp	04/09/2017 6:00:49
35195	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	LUSITANIA	Imap	11/09/2017 6:00:05
45568	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	CARTAGINENSIS	Smtp	11/09/2017 6:01:00
46572	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	CARTAGINENSIS	Imap	17/09/2017 6:00:10
47253	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	BAETICA	Smtp	17/09/2017 6:00:44
47283	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	BAETICA	Imap	17/09/2017 6:00:44
48066	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Fwd: BAETICA	Imap	17/09/2017 6:01:44
48211	192.168.47.194 [kali] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Fwd: BAETICA	Smtp	17/09/2017 6:01:49
48319	192.168.47.194 [kali] (Linux)	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Fwd: BAETICA	Imap	17/09/2017 6:01:50

También se puede ver el contenido de los correos de Juan:



Perdona, con el ansia, se me olvidÃ³ adjuntarte la imagen.

---------- Forwarded message ----------

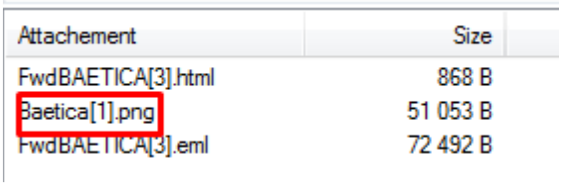
From: Juan Paredes <juanparedes@xn--metapsta-z3a.com>
Subject: BAETICA
Date: Sun, 17 Sep 2017 00:00:42 -0400
To: Elena Mellado <elenamellados@gmail.com>

Buenas noches, Elena:

Hoy te escribo nada mÃ¡s llegar de visitar un yacimiento arqueolÃ³gico
de una casa bÃ©tico romana del siglo I d.C. en Medina Sidonia, lo que
hizo acordarme de las ganas que tengo de volver a casa contigo. AllÃ-
pudimos observar restos de habitaciones, asÃ- como los criptopÃ³rticos
como el espacio que servirÃ-a de almacÃ©n de arriba, como puedes ver en
la imagen.

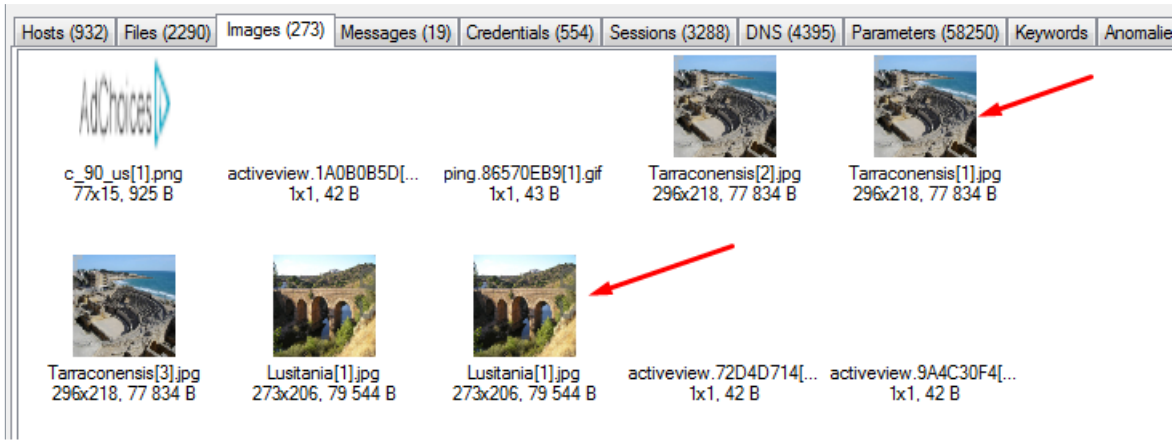
Ya espero verte en nada y acabar mi estancia y volver contigo.
Besos,
Juan

Y los adjuntos que van asociados:

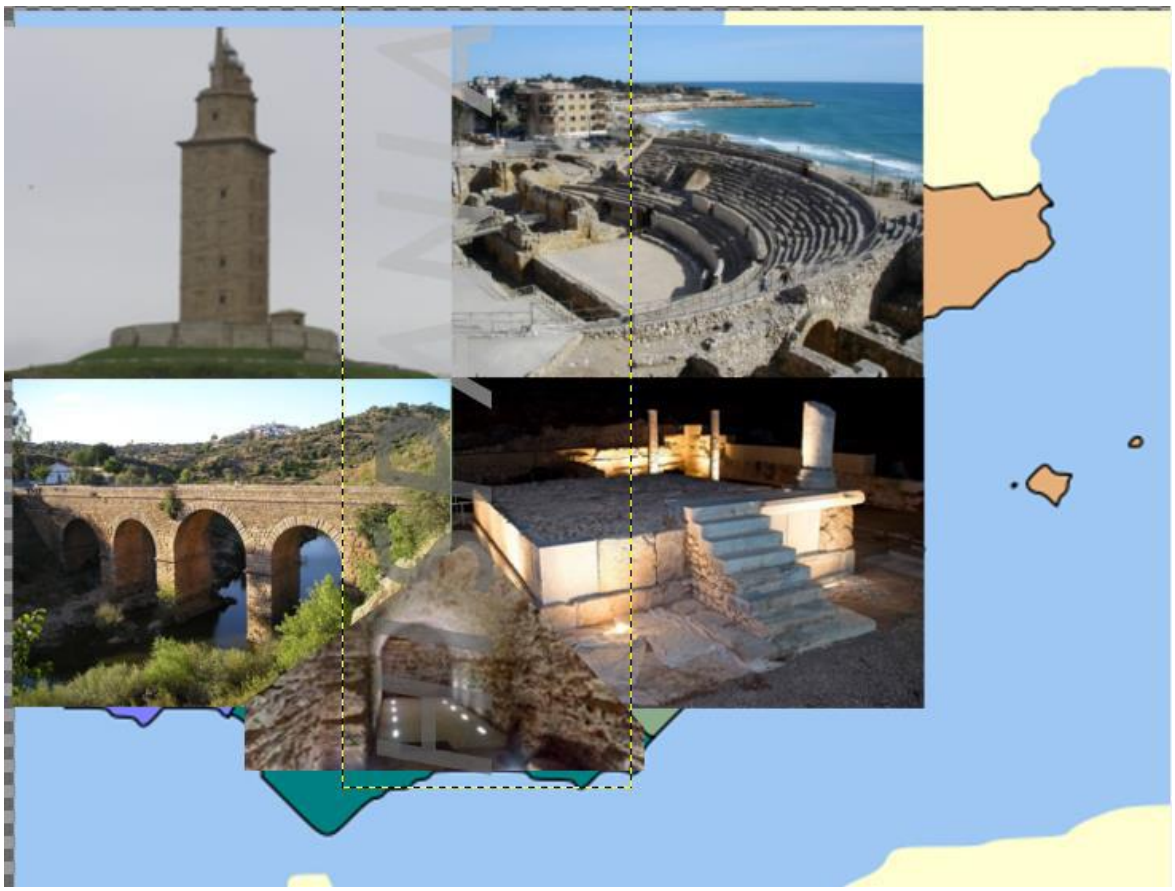


Attachement	Size
FwdBAETICA[3].html	868 B
Baetica[1].png	51 053 B
FwdBAETICA[3].eml	72 492 B

Si se recorre el hilo de correos se pueden ver los nombres de ficheros adjuntos y después buscar las imágenes entre las imágenes extraídas por NetworkMiner en la pestaña "Images":



Al recopilar las imágenes se puede juntar el puzle de la imagen global y ver el mensaje oculto:



Flag: **HISPANIA**