

Academia Hacker INCIBE

Capturas de otra época

Dificultad: **Media**

Categoría de Reto: **Forense**

Contenido

ÍNDICE DE FIGURAS	2
ÍNDICE DE TABLAS	2
1. Contexto.....	3
2. Descripción para participantes	4
3. Pistas.....	5
4. Solución	6
4.1. Opción 1.....	6
4.2. Opción 2.....	13

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.

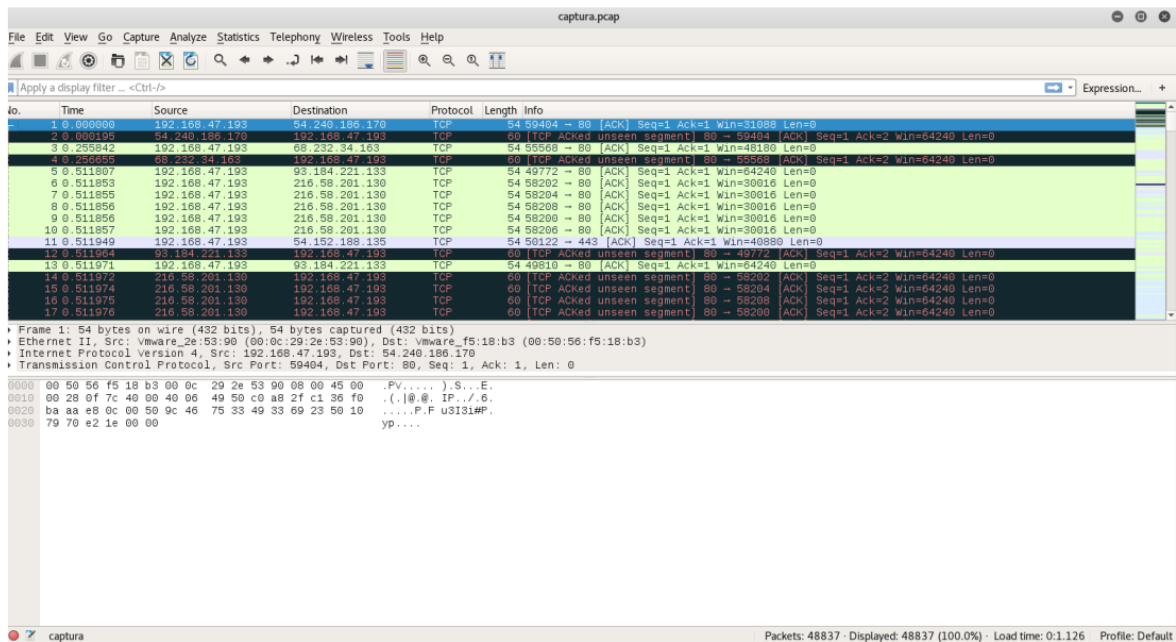
3. PISTAS

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

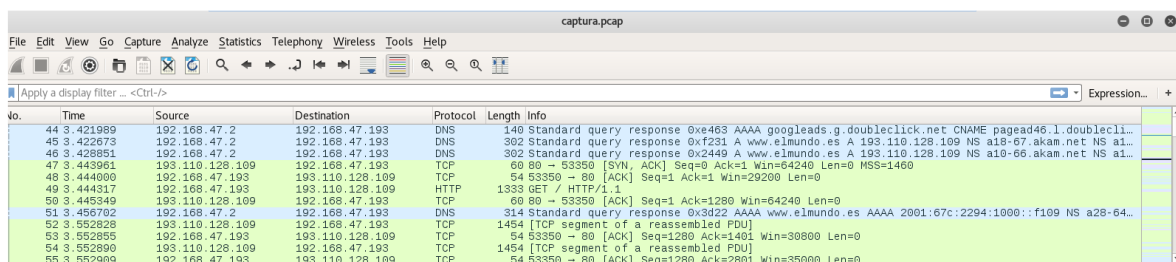
4.1. Opción 1

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.

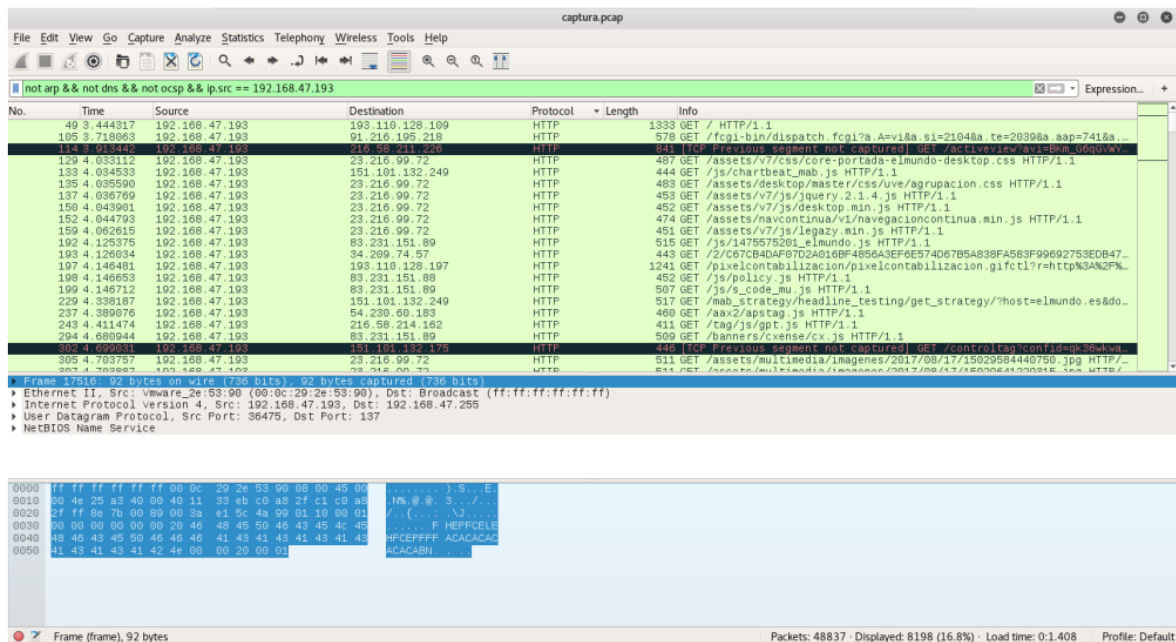
Vamos a identificar la IP del ordenador desde el que se realizan las conexiones salientes, que en este caso observamos por el intercambio de paquetes: 192.168.47.193, y se va a intentar filtrar protocolos que a priori lo único que hacen es meter ruido a la captura.



Realizamos el filtrado y después ordenamos los paquetes por protocolos:

```
not arp && not dns && not osp && 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:

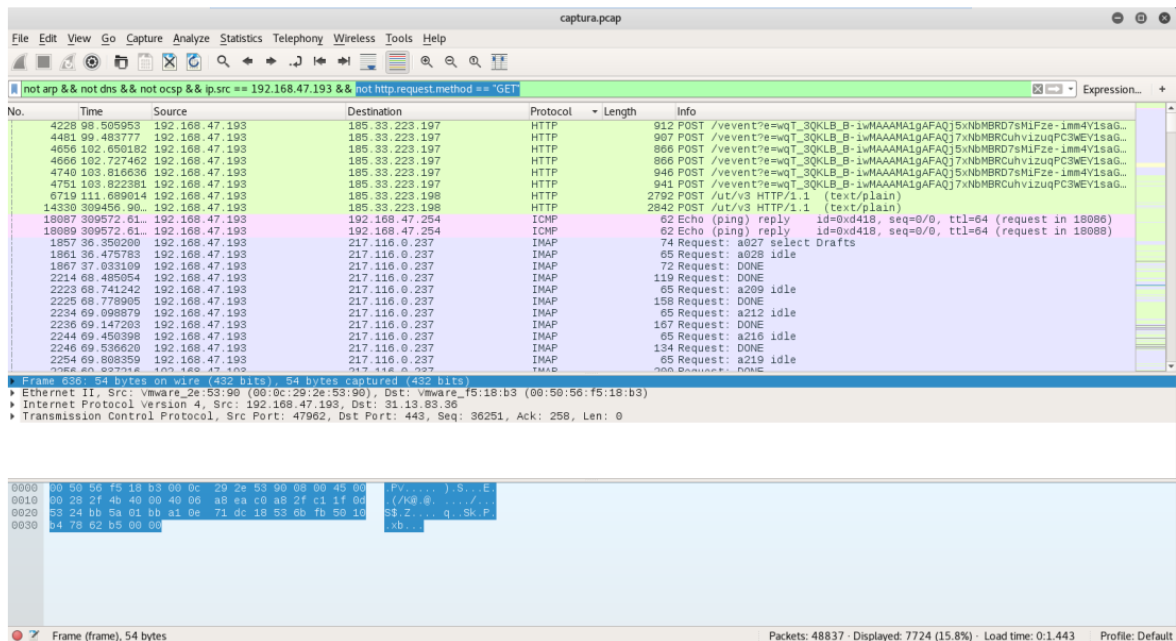


The image shows a Wireshark packet capture of traffic from source 192.168.47.193. The filter bar shows the expression: `not arp && not dns && not icmp && ip.src == 192.168.47.193`. The packet list shows numerous GET requests to various assets on the `el-mundo.es` domain. The packet details pane shows the structure of an Ethernet II frame, an Internet Protocol Version 4 header, and a User Datagram Protocol header. The packet bytes pane shows the raw hex and ASCII data of the first frame.

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

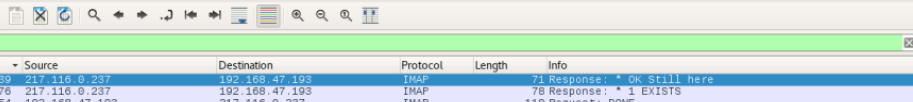
`not http.request.method == "GET"`

Quedándose la captura así:



The image shows the same Wireshark capture after applying the additional filter `not http.request.method == "GET"`. The filter bar now shows: `not arp && not dns && not icmp && ip.src == 192.168.47.193 && not http.request.method == "GET"`. The packet list shows that the HTTP GET requests have been removed, and the remaining traffic consists of IMAP protocol messages. The packet details pane shows the structure of an Ethernet II frame, an Internet Protocol Version 4 header, and a Transmission Control Protocol header. The packet bytes pane shows the raw hex and ASCII data of the first frame.

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.



The screenshot shows the Wireshark interface with a packet capture of an IMAP session. The packet list pane displays a series of IMAP commands and responses. The packet details pane shows the structure of an IMAP response, including the command, status, and body. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1879	37.576639	217.116.0.237	192.168.47.193	IMAP	71	Response: * OK Still here
2165	67.469676	217.116.0.237	192.168.47.193	IMAP	78	Response: * 1 EXISTS
2167	68.485054	217.116.0.237	192.168.47.193	IMAP	119	Request: DONE
2219	68.584952	217.116.0.237	192.168.47.193	IMAP	79	Response: *206 OK Idle completed.
2221	68.727073	217.116.0.237	192.168.47.193	IMAP	198	Response: * 1 FETCH (UID 8)
2223	68.741242	192.168.47.193	217.116.0.237	IMAP	65	Request: *209 idle
2225	68.778905	192.168.47.193	217.116.0.237	IMAP	158	Request: DONE
2227	68.841696	217.116.0.237	192.168.47.193	IMAP	64	Response: * idling
2229	68.944252	217.116.0.237	192.168.47.193	IMAP	79	Response: *209 OK Idle completed.
2231	69.896449	217.116.0.237	192.168.47.193	IMAP	282	Response: * 1 FETCH (UID 8 BODY(HEADER.FIELDS (FROM REPLY-TO SENDER...
2234	69.908879	192.168.47.193	217.116.0.237	IMAP	65	Request: *212 idle
2236	69.147263	192.168.47.193	217.116.0.237	IMAP	167	Request: DONE
2239	69.197215	217.116.0.237	192.168.47.193	IMAP	64	Response: * idling
2240	69.295989	217.116.0.237	192.168.47.193	IMAP	79	Response: *212 OK Idle completed.
2242	69.434574	217.116.0.237	192.168.47.193	IMAP	586	Response: * 1 FETCH (UID 8 ENVELOPE ("Thu, 17 Aug 2017 16:04:06 +02...
2244	69.450398	192.168.47.193	217.116.0.237	IMAP	65	Request: *216 idle
2246	69.536620	192.168.47.193	217.116.0.237	IMAP	134	Request: DONE
2248	69.554394	217.116.0.237	192.168.47.193	IMAP	64	Response: * idling
2250	69.663941	217.116.0.237	192.168.47.193	IMAP	79	Response: *216 OK Idle completed.
2252	69.743905	217.116.0.237	192.168.47.193	IMAP	401	Response: * 1 FETCH (UID 8 BODY[1]<=> {128
2254	69.808359	192.168.47.193	217.116.0.237	IMAP	65	Request: *210 idle
2256	69.897516	192.168.47.193	217.116.0.237	TLSv1.2	300	Request: DONE

Packet 1879: Ethernet II, Src: Vmware, Dst: Vmware, Length: 71 bytes, Info: 71 bytes captured on interface eth0

Packet 2256: Ethernet II, Src: Vmware, Dst: Vmware, Length: 300 bytes, Info: 300 bytes captured on interface eth0

Packet 2256 details: Ethernet II, Src: Vmware, Dst: Vmware, Length: 300 bytes, Info: 300 bytes captured on interface eth0

Packet 2256 details: Internet Protocol version 4, Src: 217.116.0.237, Dst: 192.168.47.193

Packet 2256 details: Transmission Control Protocol, Src Port: 143, Dst Port: 37032, Seq: 1, Ack: 1, Len: 17

0000 20 0c 29 2e 53 00 00 00 55 15 18 b3 00 00 45 00 .).S.P.v...E
0001 00 30 14 b7 00 00 00 06 7b 3c 09 74 00 00 c0 a8 9...c...t...
0002 2f c1 00 8f 00 a8 63 c2 10 00 ec 69 38 bd 50 18 ...c...18.P
0003 fa f0 50 62 00 00 2a 20 4f 4b 20 53 74 69 6c 6c Pb... OK Still
0004 20 69 65 72 65 00 00 here

Frame (frame): 71 bytes Packets: 48837 · Discarded: 816 (1.7%) · Load time: 0:0.782 Profile: Default

```
a027 select Drafts
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1502955652] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
a027 OK [READ-WRITE] Select completed (0.001 secs).
a028 idle
+ idling
DONE
a029 close
a028 OK Idle completed.
a029 OK Close completed.
a030 select Drafts
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 0 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1502955652] UIDs valid
* OK [UIDNEXT 2] Predicted next UID
a030 OK [READ-WRITE] Select completed (0.000 secs).
a031 idle
+ idling
DONE
a032 close
a031 OK Idle completed.
a032 OK Close completed.
a033 select Sent
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft \*)] Flags permitted.
* 3 EXISTS
* 0 RECENT
* OK [UIDVALIDITY 1502955653] UIDs valid
* OK [UIDNEXT 4] Predicted next UID
a033 OK [READ-WRITE] Select completed (0.000 secs).
a034 idle
DONE
a035 append Sent (\seen) {8906}
+ idling
Date: Thu 17 Aug 2017 10:05:26 -0400
37 client pkts, 42 server pkts, 55 turns.
```

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.

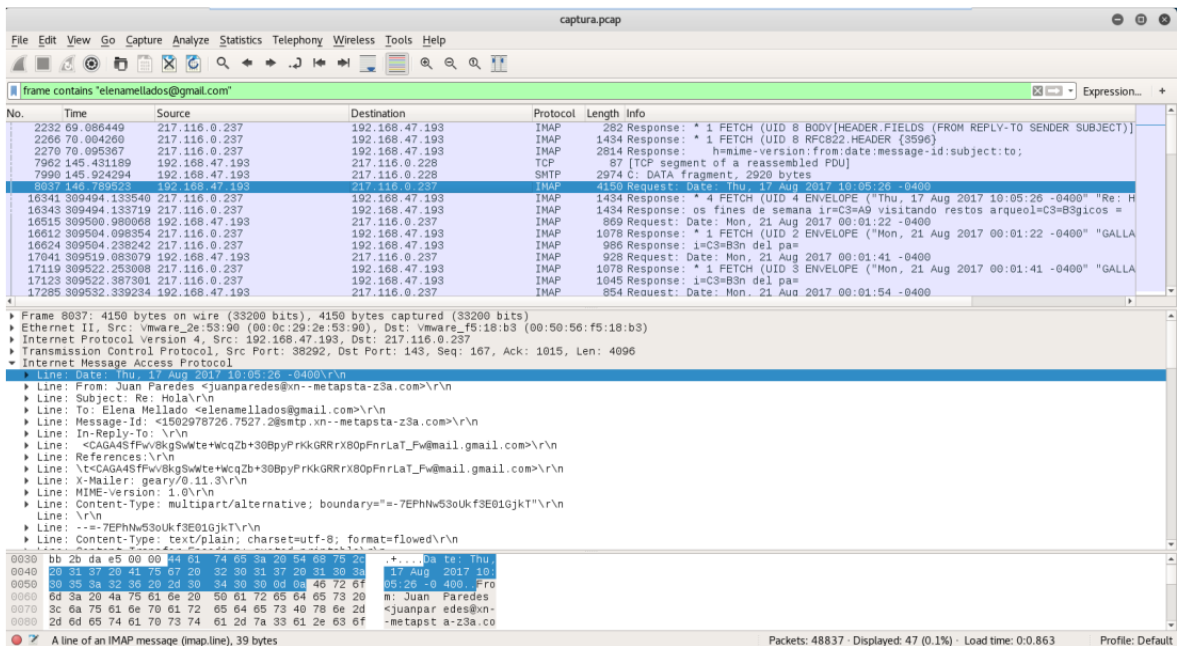
```
Wireshark · Follow TCP Stream (tcp.stream eq 104) · captura

<div>Hola Elena:&nbsp;  </div><div><br></div><div>Aquí estoy bien y voy =
avanzando cada día. De hecho, durante los próximos fines de semana
iré visitando restos arqueológicos de cada una de las divisiones
administrativas que llevaron a cabo Diocleciano durante la época romana,
aunque, en esa época, la innovación más importante que se hizo fue la
creación de las llamadas diócesis. Ya sabes que soy un fanático de la
historia romana. Te mandaré un correo con distintas fotos de lo más
destacado de cada una, pero no te olvides de apreciarla maravilla de los
monumentos.&nbsp;  </div><div>Yo también te echo de menos.&nbsp;  </div>
<div><br></div><div>Un beso,&nbsp;  </div><div><br></div><div>Tu Juan&nbsp;  </div>
<br>On Thu, Aug 17, 2017 at 10:04 AM, Elena Mellado <elenamellados@gmail.com> wrote:
<blockquote type="cite"><div dir="ltr"><div class="gmail-OutlineElement gmail-Ltr gmail-SCXW127867301" style="margin:0px;padding:0px;overflow:visible;clear:both;direction:ltr;color:rgb(0,0,0);font-family:"&quot;Segoe UI&quot;;font-size:12px"><p class="gmail-Paragraph gmail-SCXW127867301" style="margin:0px;padding:0px;word-wrap:break-word;vertical-align:baseline;background-color:transparent;color:windowtext"><span class="gmail-TextRun gmail-SCXW127867301" lang="ES" style="margin:0px;padding:0px;color:rgb(34,34,34);font-size:9.5pt;font-family:Arial,Helvetica,MSFontService,sans-serif;line-height:16px;font-variant-ligatures:none"><span class="gmail-NormalTextRun gmail-SCXW127867301" style="margin:0px;padding:0px;background-color:inherit">Hola cari:</span><span class="gmail-EOP gmail-SCXW127867301" style="margin:0px;padding:0px;font-size:9.5pt;line-height:16px;font-family:Arial,Helvetica,MSFontService,sans-serif">&nbsp;</span></div><div class="gmail-OutlineElement gmail-Ltr gmail-SCXW127867301" style="margin:0px;padding:0px;overflow:visible;clear:both;direction:ltr;color:rgb(0,0,0);font-family:"&quot;Segoe UI&quot;;font-size:12px"><p class="gmail-Paragraph gmail-SCXW127867301" style="margin:0px;padding:0px;word-wrap:break-word;vertical-align:baseline;background-color:transparent;color:windowtext"><span class="gmail-TextRun gmail-SCXW127867301" lang="ES" style="margin:0px;padding:0px;color:rgb(34,34,34);font-size:9.5pt;font-family:Arial,Helvetica,MSFontService,sans-serif;line-height:16px;font-variant-ligatures:none"><span class="gmail-NormalTextRun gmail-SCXW127867301" style="margin:0px;padding:0px;background-color:inherit">=C2=BFQu=3=A9 tal est=3=A1s? Espero que lo est=3=A9s pasando bien por España. =C2=BFHay alguna novedad? Por aquí =AD estamos impacientes por saber más de ti. Espero que nos vayas informando de las novedades.</span></span><span class="gmail-EOP gmail-SCXW127867301" style="margin:0px;padding:0px;font-size:9.5pt;line-height:16px;font-family:Arial,Helvetica,MSFontService,sans-serif">&nbsp;</span></div></div></div>

Packet 8037. 37 client pkts, 42 server pkts, 55 turns. Click to select.
Entire conversation (21 kB) Show and save data as ASCII Stream 104
Find: Find Next
Help Filter Out This Stream Print Save as... Back Close
```

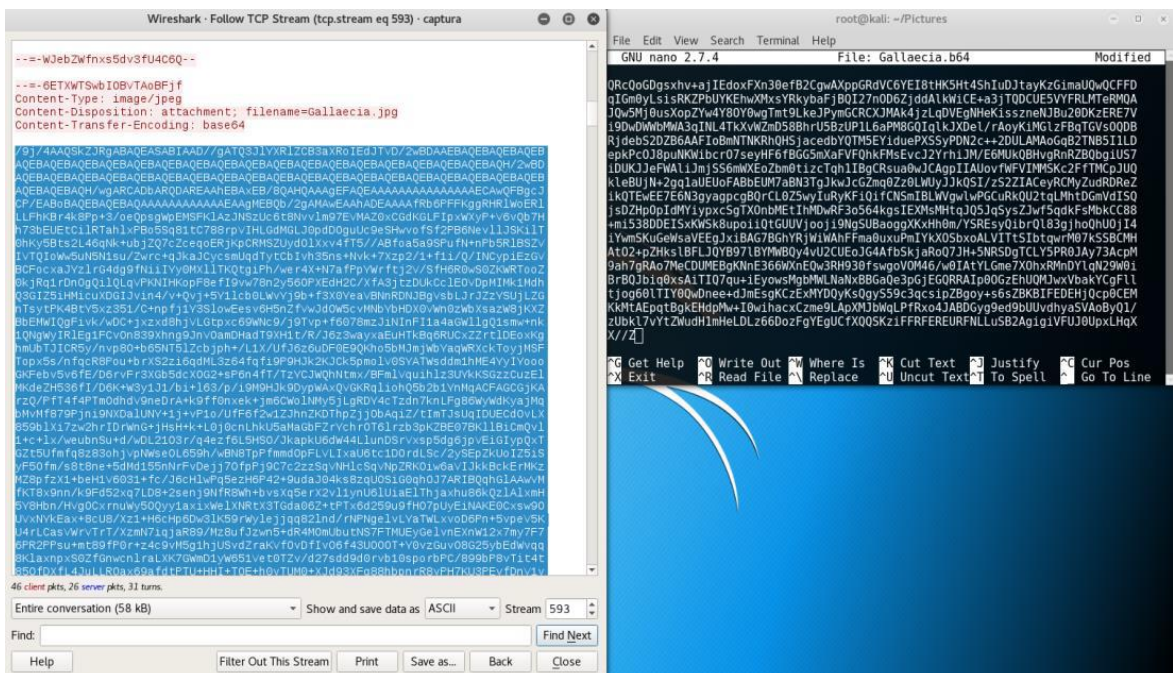
Ahora vamos a filtrar entre los paquetes que se dirijan a Elena:

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
```

```
root@kali: ~/Pictures
File Edit View Search Terminal Help
bash: Nano: command not found
root@kali:~# ls
captura.pcap  Documents  Music      Public     Videos
Desktop       Downloads  Pictures   Templates
root@kali:~# cd Pictures/
root@kali:~/Pictures# nano Gallaecia.b64
root@kali:~/Pictures# base64 -d Gallaecia.b64 > Gallaecia.jpeg
root@kali:~/Pictures#
```

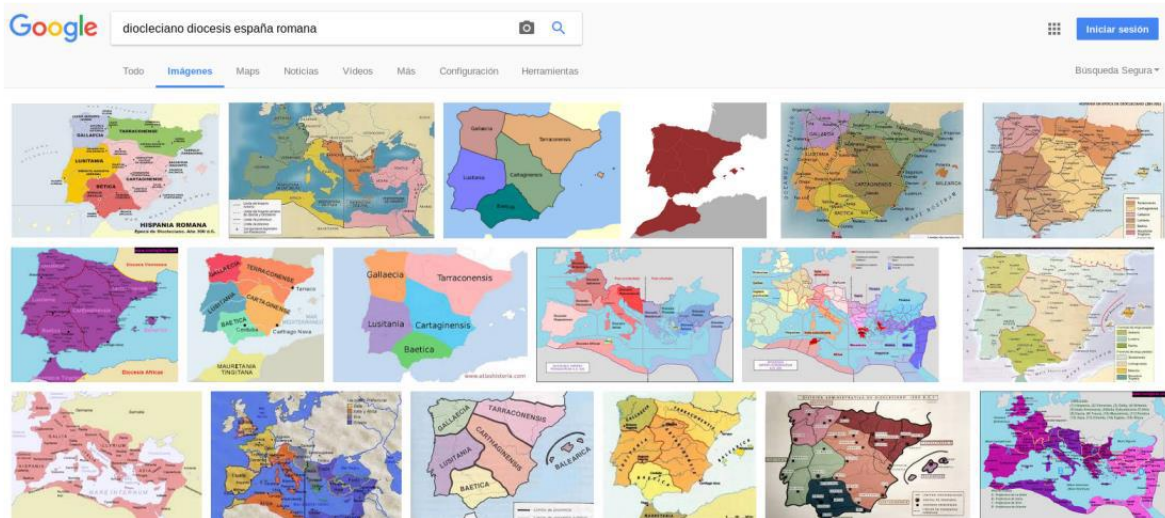
Y obtenemos nuestra imagen:



Repetimos la misma operación para cada una de las imágenes.

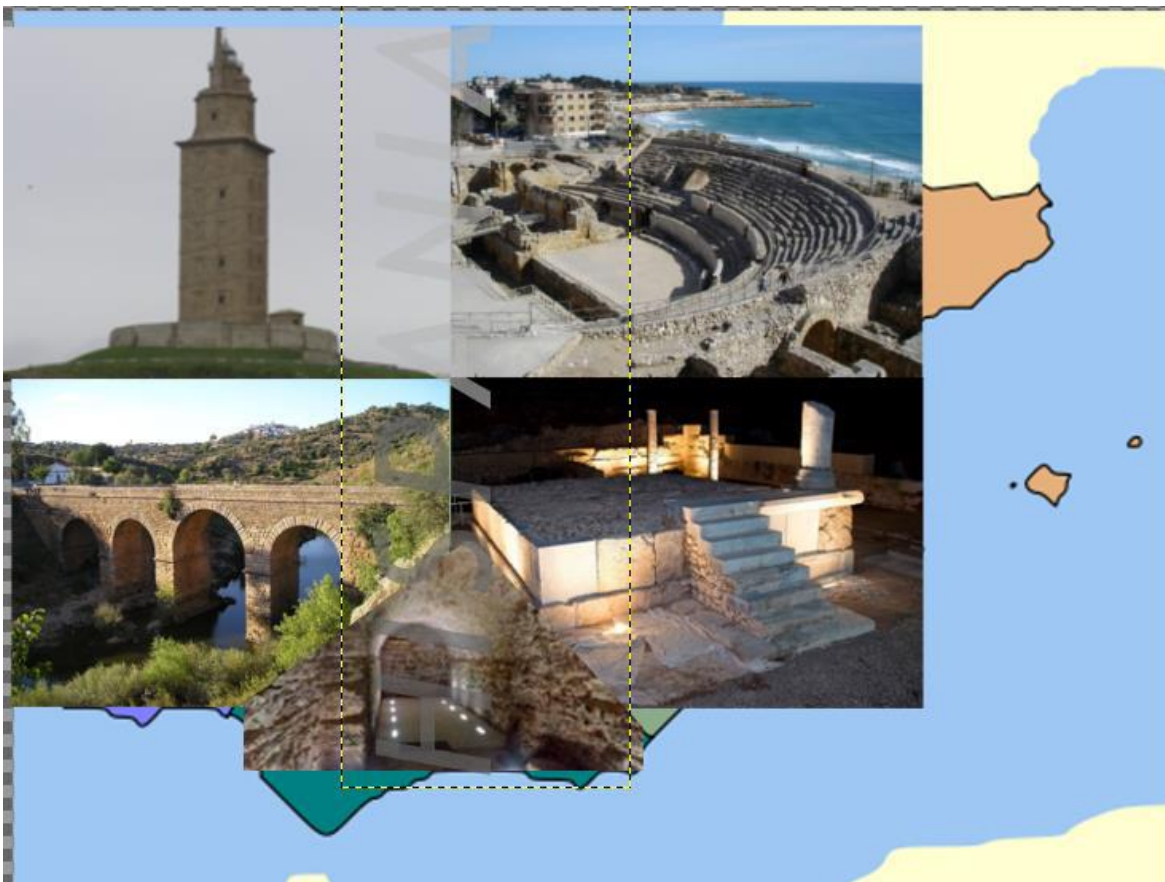
GALLAECIA, TARRACONENSIS, LUSITANIA, CARTAGINENSIS y BAETICA.

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:

NetworkMiner 2.1.1

File Tools Help

Select a network adapter in the list ---

Hosts (932) Files (2290) Images (273) Messages (19) Credentials (554) Sessions (3288) DNS (4395) Parameters (58250) Keywords / Anomalies

Filter keyword: ☐ Case sensitive ☐ ExactPhrase

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	Smtpt	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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECIA	Smtpt	21/08/2017 6:03:16
18627	192.168.47.194 [kall] (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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	TARRACONENSIS	Smtpt	28/08/2017 6:01:25
32577	192.168.47.194 [kall] (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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	LUSITANIA	Smtpt	04/09/2017 6:00:49
35195	192.168.47.194 [kall] (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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	CARTAGINENSIS	Smtpt	11/09/2017 6:01:00
46572	192.168.47.194 [kall] (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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	BAETICA	Smtpt	17/09/2017 6:00:44
47283	192.168.47.194 [kall] (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 [kall] (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 [kall] (Linux)	217.116.0.228	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	Fwd: BAETICA	Smtpt	17/09/2017 6:01:49
48319	192.168.47.194 [kall] (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 olvidó 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 más llegar de visitar un yacimiento arqueológico de una casa báltico romana del siglo I d.C. en Medina Sidonia, lo que hizo acordarme de las ganas que tengo de volver a casa contigo.

Allí pudimos observar restos de habitaciones, así como los criptoárticos como el espacio que servía de almacén de amiba, como puedes ver en la imagen.

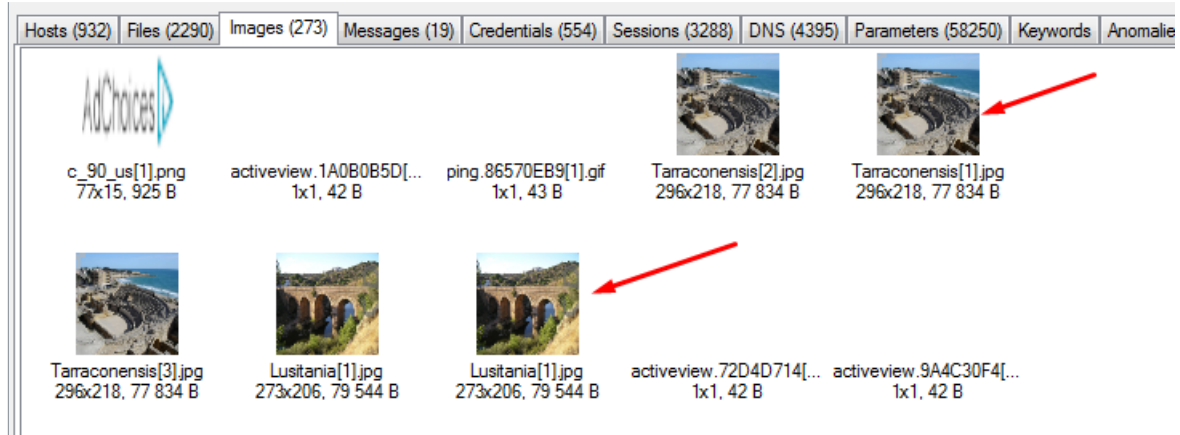
Ya espero verte en nada y acabar mi estancia y volver contigo.

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 puzzle de la imagen global y ver el mensaje oculto:



Flag: **HISPANIA**