



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_

Academia Hacker INCIBE

Capturas de otra época

Dificultad: Media

Categoría de Reto: Forense

 incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD





GOBIERNO

DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITALSECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

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.



GOBIERNO

DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



1. CONTEXTO

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

Flag: **HISPAÑIA**

Datos Proporcionados:

- Archivo .pcap



GOBIERNO

DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNOMINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITALSECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

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.



GOBIERNO

DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



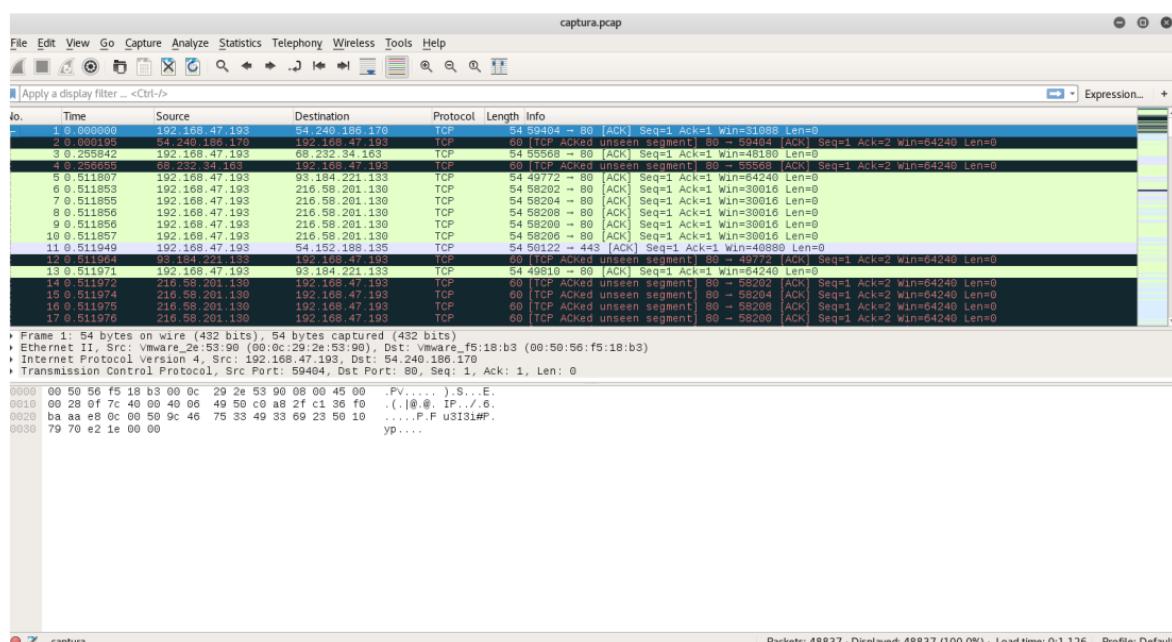
3. PISTAS

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

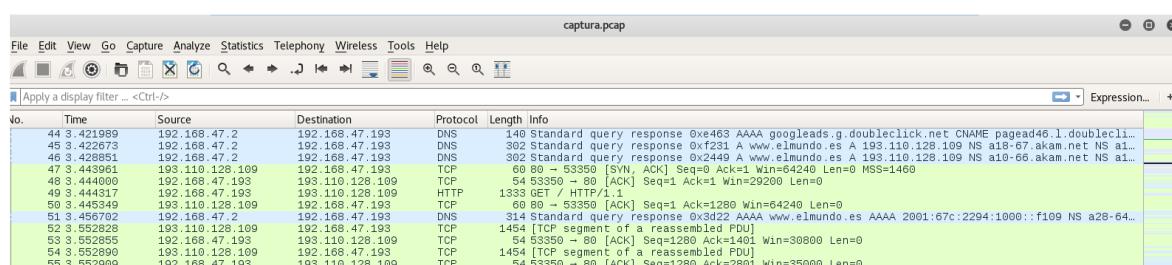
4.1. Opción 1

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:

The screenshot displays a Wireshark interface with the following key elements:

- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**: The top menu bar.
- captura.pcap**: The current file being analyzed.
- not arp & not dns & not oscp & ip.src == 192.168.47.193**: The selected display filter.
- Expression... +**: A search bar for entering additional filters.
- No. Time Source Destination Protocol Length Info**: The column headers for the packet list.
- Packet List**: Shows approximately 1000 captured packets, mostly from 192.168.47.193 to various destinations like 192.168.47.193, 192.168.47.192, and 192.168.47.194. Many are HTTP GET requests for static files.
- Details**: Provides a detailed view of the selected packet's structure, including hex, ASCII, and decimal representations.
- Bytes**: Shows the raw binary data of the selected packet.

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 screenshot shows the Wireshark interface with the following details:

- Frame List:** Shows 48837 total frames, with frame 636 selected.
- Selected Frame (Frame 636):**
 - Summary:** Ethernet II, Src: Vmware_2e [53:90 (00:0c:29:2e:53:90)], Dst: Vmware_f5 [18:03 (00:05:56:f5:18:b3)]
 - Details:** Internet Protocol Version 4, Src Port: 47962, Dst Port: 443, Seq: 36251, Ack: 258, Len: 0
 - Hex:** 0000 00 50 56 56 16 b3 60 0c 29 2e 53 99 68 00 45 00 |Pv.....).S. E.|
0010 00 25 2f 4b 49 00 40 06 28 eh c0 a8 2f c1 ff 0d |W@ @. / . . .|
0020 53 24 hb 5a 61 bb 01 ee 71 dc 18 53 6b fb 50 10 |\$1.2... q. Sk P.|
0030 04 78 62 bb 00 00 00 00 00 00 00 00 00 00 00 00 00 |vb ..|
- Bottom Panel:** Shows the packet details, bytes, and error columns.

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.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

imap

No.	Time	Source	Destination	Protocol	Length	Info
1	18:00:59.717,116.0.237	217.116.0.237	192.168.47.193	IMAP	71	Response: * Ok Still here
2	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	78	Response: * EXISTS
3	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	110	Request: DONE
4	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	118	Response: a206 OK Idle completed.
5	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	198	Response: * 1 FETCH (UID 8)
6	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	65	Request: a209 idle
7	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	156	Request: DONE
8	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	64	Response: + idling
9	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	79	Response: a209 Idle completed.
10	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	282	Response: * 1 FETCH (UID 8 BODY[HEADER.FIELDS (FROM REPLY-TO SENDER...]
11	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	65	Request: a212 idle
12	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	167	Request: DONE
13	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	64	Response: + idling
14	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	79	Response: a212 Idle completed.
15	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	586	Response: * 1 FETCH (UID 8 ENVELOPE ("Thu, 17 Aug 2017 16:04:06 +02...)
16	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	65	Request: a216 idle
17	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	134	Request: DONE
18	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	64	Response: + idling
19	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	79	Response: a216 OK Idle completed.
20	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	409	Response: * 1 FETCH (UID 8 BODY[1]<0> {128}
21	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	65	Request: a219 idle
22	18:00:59.717,116.0.237	192.168.47.193	217.116.0.237	IMAP	66	Response: DONE

Frame 18/9: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)
 ▶ Ethernet II, Src: VMware_4f:18:b3 (00:50:56:f5:18:b3), Dst: VMware_4f:18:b3 (00:0c:29:2e:53:90)
 ▶ Internet Protocol Version 4, Src: 217.116.0.237, Dst: 192.168.47.193
 ▶ Transmission Control Protocol, Src Port: 145, Dst Port: 37032, Seq. 1, Ack: 1, Len: 17
 ▶ Internet Message Access Protocol

Frame (frame), 71 bytes

Packets: 48837 · Displayed: 816 (1.7%) · Load time: 0:0.782 · Profile: Default

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

```
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.
```

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

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: </div><div>
</div><div>Aqui estoy bien y voy = avanzando cada d=C3=ADa. De hecho, durante los pr=C3=B3ximos fines de semana ir=C3=A9 visitando restos arqueol=C3=B3gicos de cada una de las divisiones administrativas que llev=C3=A9n a cabo Diocleciano durante la =C3=A9poca romana, aunque, en esa =C3=A9poca, la innovaci=C3=B3n m=C3=A1s importante que hizo fue la creaci=C3=B3n de las llamadas di=C3=B3cesis. Ya sabes que soy un fan=C3=A1tico de la historia romana. Te mandar=C3=A9 un correo con distintas fotos de lo m=C3=A1s destacado de cada una, cont=C3=A1ndote un poco sobre historia, pero no te olvides de apreciarla maravilla de los monumentos. </div><div>
</div><div>Yo tambi=C3=A9n te echo de menos. </div><div>
</div><div>Un beso, </div><div>
</div>Tu Juan </div>
On Thu, Aug 17, 2017 at 10:04 AM, Elena Mellado <elenamellados@gmail.com> wrote:
<blockquote type=3D"cite"><div dir=3D"ltr"><div class=3D"gmail-OutlineElement gmail-Ltr gmail-gmail-SCXW127867301" style=3D"margin:0px;padding:0px;overflow:hidden;clear:both;direction:ltr;color:rgb(0,0,0);font-family:"Segoe UI","Arial,"Verdana,sans-serif;font-size:12px"><p class=3D"gmail-Paragraph gmail-gmail-SCXW127867301" style=3D"margin:0px;padding:0px;word-wrap:break-word;vertical-align:baseline;background-color:transparent;color:windowtext">= Hola cari=C3=B1o: </p></div><div class=3D"gmail-OutlineElement gmail-Ltr gmail-gmail-SCXW127867301" style=3D"margin:0px;padding:0px;overflow:visible;clear:both;direction:ltr;color:rgb(0,0,0);font-family:"Segoe UI","Arial,"Verdana,sans-serif;font-size:12px"><p class=3D"gmail-Paragraph gmail-gmail-SCXW127867301" style=3D"margin:0px;padding:0px;word-wrap:break-word;vertical-align:baseline;background-color:transparent;color:windowtext">=C2=BFQu=C3=A9 tal est=C3=A9? Espero que lo est=C3=A9 pasando bien por Espa=C3=B1a. =C2=BFHay alguna novedad? Por aqu=C3=A9=AD estamos impacientes por saber m=C3=A1s de ti. Espero que nos vayas informando de las novedades. </p></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

The screenshot shows a Wireshark capture of an IMAP session. The interface includes a top bar with file, edit, view, go, capture, analyze, statistics, telephony, wireless, tools, help, and expression search options. The main window displays a list of network frames, with frame 8037 highlighted. The details pane shows the IMAP protocol structure, and the bytes pane shows the raw binary data. A status bar at the bottom indicates the number of packets (48837), displayed packets (47), load time (0.0863 seconds), and profile (Default).

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.

The figure shows two windows side-by-side. The left window is Wireshark displaying a TCP stream (tcp.stream eq 593) with 46 client ppts, 26 server ppts, and 31 turns. The right window is a terminal session titled 'File: Gallaecia.b64' with the command 'root@kali: ~/Pictures'. The terminal output shows the file being decoded from base64.

```

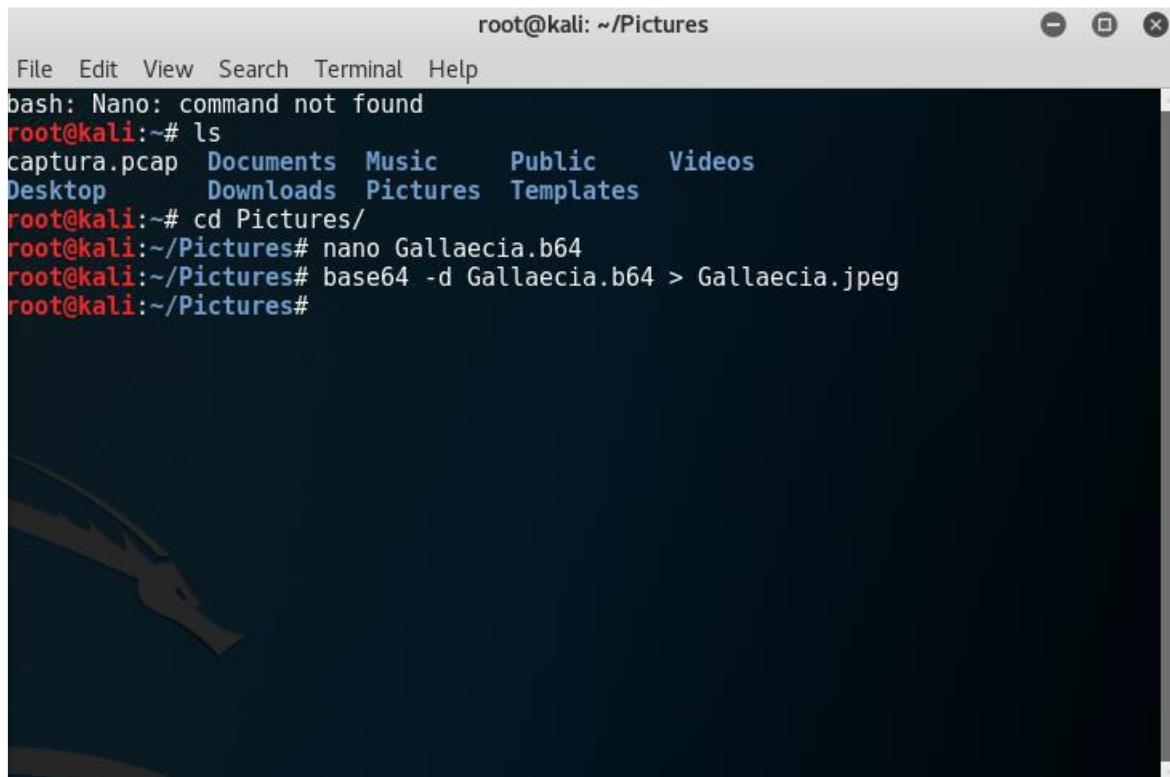
Wireshark - Follow TCP Stream (tcp.stream eq 593) - capture
File Edit View Search Terminal Help
File GNU nano 2.7.4 File: Gallaecia.b64 Modified
0RQoGdsGws+ajIEDoxFx30eBfZCwAxppGRvC6YIE18tHK5h45hDjTayKzGimaU0QjFFD
qIGm8yLisrKZPbUYKeHwXmsRYkybaFjBQ127n0dZ6ddalKwICE+A3jTQDCUEVYFRLMterMOA
Jw5MjusXopZpY708Wyo9WmgT9kLePmcyCRMCMAkjLgQlVegNeHkisszneBvBz0DzTEREV
i9wdbWMDWA3qINL4TkWznD8BjU5BjLp6AgQlQkFBgV500QDB
RjdeB26BAAf0Ib0MnTRNKR0Hs)adbdYOTMSEyuePSXSyP0N2c+-+2DLAnAgQgB2TN811LD
epkPcOJ8unKmWb1cr07seyHF6Gm5xaF0kHFMx7Dy2Jy1JAM_E6MkHgByHrvRzB0bg1J
LUDKjE1JLjS56mXe0o7tzcTqH1BgRsua0WJAgpJ1ALJovyF27TmPjJQ
KleBuN+2g2lalMaB7E8BfEM7Ab3TgJkWqzGm0zZ8L0WjJk0S1/z52TAceyRCyMuZdrReZ
Lk0TEWeE7E6N3ygaagcB0tCL82wy1UrYKf101TNSBLVWgw1PgURkU02tLmhDgMdMs1Q
jsdZPh0p1ldMyplsgxTx0nDtE1MhDRf3o564kg1TeXMsMhtJ051q5ysZjWtSqdkrsMbCc88
+m53280DEISXyWb8pu01TgJU00po1j9ng5UbaoaggKXxh0mHSREsybrj183gjhoh0U14
LyWmsKuGeWaEegJyBaG7B6y1WlWAhFmaeuixpJYtX0SbxoALV1T7sbtqwm97ksBCBMM
At2+PzKs1BFJ0y897tBYMwB0y4V2ZUEoJ4AfAb5k1r0o7JH-5N5dgTCLSPR0Aj7y3acPm
9ah7gRa0MDeDMBEGKRNnE366wxEw03RH938tswgv0M46/w1AtLYmz7X0nhRmDyLqN29w6i
BrBQjB1q9asX11T07qu1EyowMgbMLNaB8B6e3p9gEGQRRA1p06zehU0MjVbaYKcgFl
tjog601T1W0Dnee+djMsEgkCExMYDyKs0gy559-3qscipZBgoY+s6z8Bk1FEDHjCqpcBEM
KMTAEPqBgeHdpN+10w1haxczme91ApXH0qLPrR0x4jABDdg9ye9jb0Uvhdy5VAoBy1
zubk1VytZwd1HmheDL26d0zg7YEGut0QSK21FRFERURFNLUSB2Aq1GVFU0jUpLhQx
X/4]

Get Help Write Out Where Is Cut Text Justify Cur Pos
Exit Read File Replace Uncut Text To Spell Go To Line

```

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

```
# base64 -d Gallaecia.bs64 > Gallaecia.jpeg
```



The terminal window shows the following session:

```
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#
```

The terminal window has a dark background with light-colored text. It shows the user is in the root directory of the Pictures folder. The user runs the command `base64 -d Gallaecia.b64 > Gallaecia.jpeg` to decode the base64 encoded image and save it as `Gallaecia.jpeg`.

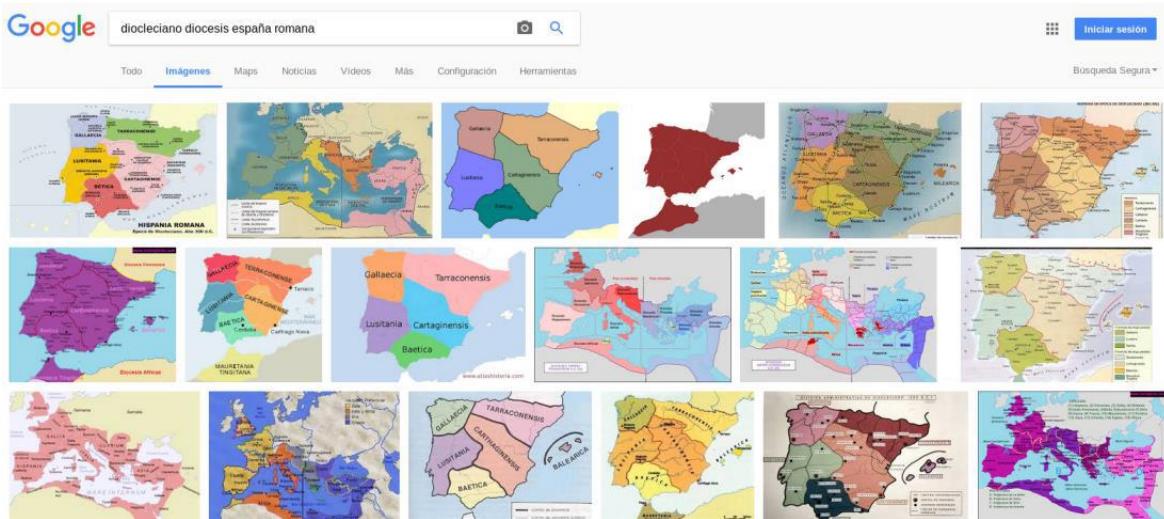
Y obtenemos nuestra imagen:



Repetimos la misma operación para cada una de las imágenes.

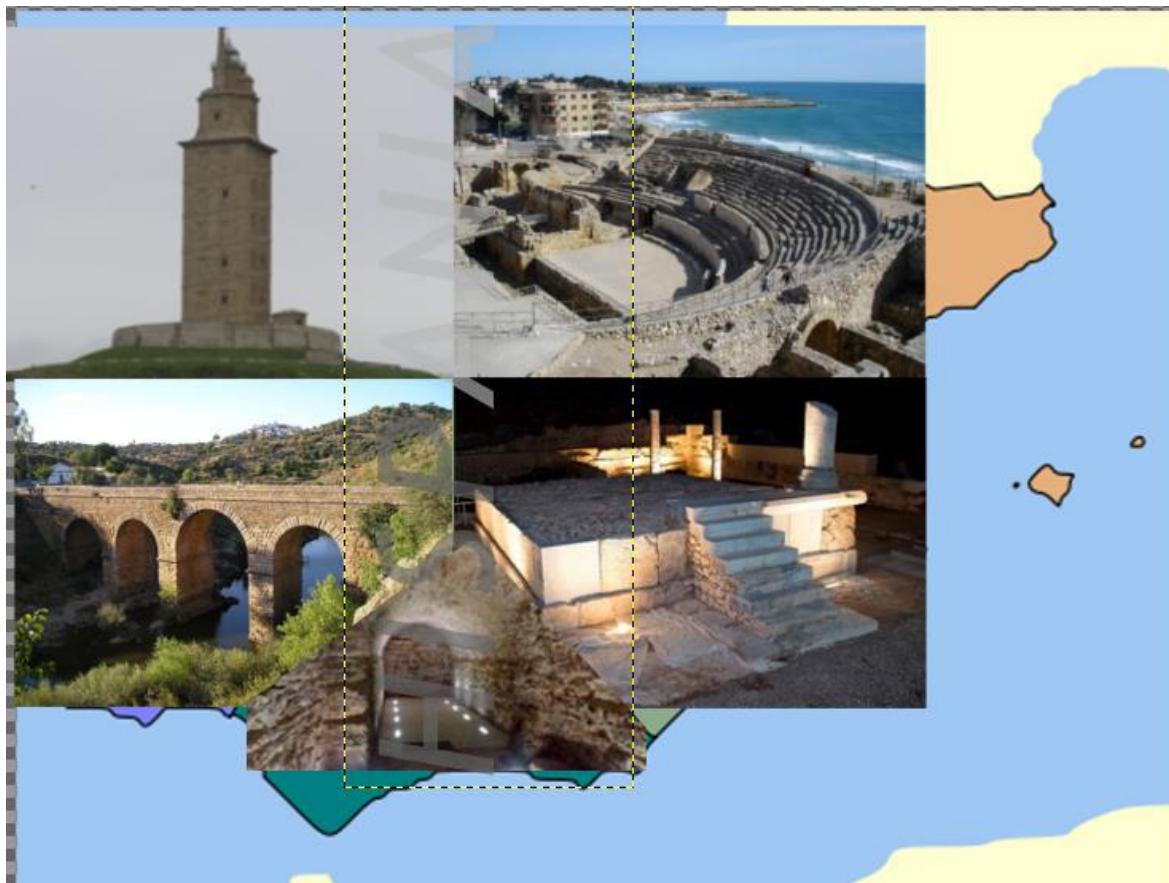
GALLAECIA, TARRACONENSIS, LUSITANIA, CARTAGINENSIS y BAETICA.

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	Sntp	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
16615	192.168.47.193	217.116.0.237	Juan Paredes <juanparedes@xn--metapsta-z3a.com>	Elena Mellado <elenamellados@gmail.com>	GALLAECA	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>	GALLAECA	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>	GALLAECA	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>	GALLAECA	Sntp	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>	GALLAECA	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	Sntp	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	Sntp	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	Sntp	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	Sntp	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	Sntp	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 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:

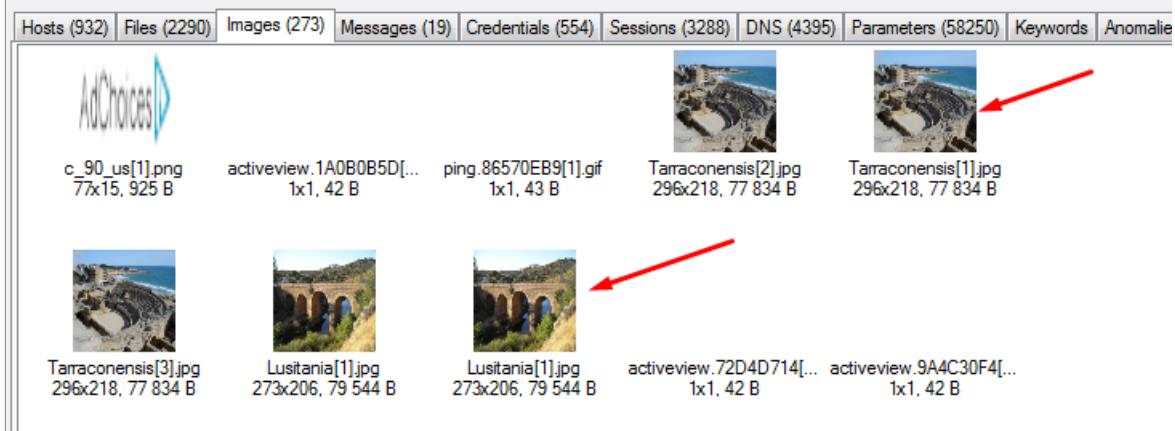
Hoy te escribo nada más llegar de visitar un yacimiento arqueológico de una casa baética romana del siglo I d.C. en Medina Sidonia, lo que hizo acordarme de las ganas que tengo de volver a casa contigo. Allá pudimos observar restos de habitaciones, así como los criptopórticos como el espacio que serviría de almacén 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”:

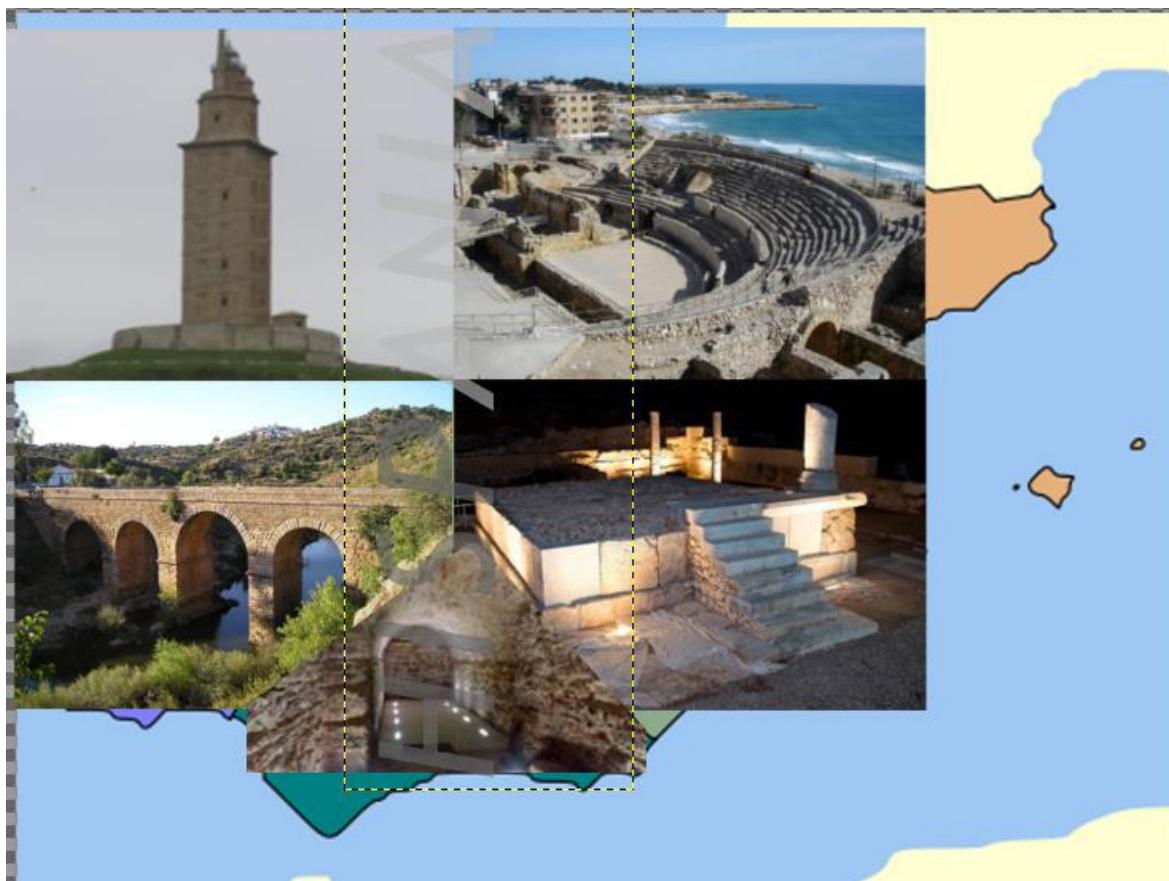


Hosts (932) | Files (2290) | Images (273) | Messages (19) | Credentials (554) | Sessions (3288) | DNS (4395) | Parameters (58250) | Keywords | Anomalies

c_90_us[1].png 77x15, 925 B activeview.1A0B0B5D[... 1x1, 42 B ping.86570EB9[1].gif 1x1, 43 B Tarraconensis[2].jpg 296x218, 77 834 B Tarraconensis[1].jpg 296x218, 77 834 B

Tarraconensis[3].jpg 296x218, 77 834 B Lusitania[1].jpg 273x206, 79 544 B Lusitania[1].jpg 273x206, 79 544 B activeview.72D4D714[... 1x1, 42 B activeview.9A4C30F4[... 1x1, 42 B

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



Flag: **HISPANIA**