



Sub-task 1:

- anz-logo.jpg and bank-card.jpg are two images that show up in the users network traffic.
- Extract these images from the pcap file and attach them to your report.

First of all I'm going to filter only the HTTP traffic:

No.	Time	Source	Destination	Protocol	Length	Info
1	131.6.132470	::1	::1	HTTP	402	GET /anz-logo.jpg HTTP/1.1
2	1363216	::1	::1	HTTP	1065	HTTP/1.1 200 OK (JPEG JFIF image)
3	505 22.697209	::1	::1	HTTP	403	GET /bank-card.jpg HTTP/1.1
4	567 24.333701	::1	::1	HTTP	348	HTTP/1.1 200 OK (JPEG JFIF image)
5	818 36.266571	::1	::1	HTTP	401	GET /anz-png.png HTTP/1.1
6	827 36.412652	::1	::1	HTTP	790	HTTP/1.1 200 OK (PNG)
7	1051 46.737160	::1	::1	HTTP	389	GET /how-to-commit-crimes.docx HTTP/1.1
8	1077 47.744581	::1	::1	HTTP	488	HTTP/1.1 200 OK (application/vnd.openxmlformats-officedocument.wordprocessingml.document)
9	1263 55.003920	::1	::1	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
10	1337 56.697723	::1	::1	HTTP	1453	HTTP/1.1 200 OK (text/plain)
11	1552 66.669786	::1	::1	HTTP	609	GET /evil.pdf HTTP/1.1
12	1598 67.704563	::1	::1	HTTP	1486	HTTP/1.1 200 OK (application/pdf)
13	1774 75.599414	::1	::1	HTTP	403	GET /atm-image.jpg HTTP/1.1
14	1796 75.906854	::1	::1	HTTP	352	HTTP/1.1 200 OK (JPEG JFIF image)
15	2085 89.620153	::1	::1	HTTP	617	GET /ANZ_Document.pdf HTTP/1.1
16	2537 97.648691	::1	::1	HTTP	1284	HTTP/1.1 200 OK (application/pdf)
17	2662 103.007294	::1	::1	HTTP	618	GET /ANZ_Document2.pdf HTTP/1.1
18	3522 112.142837	::1	::1	HTTP	744	HTTP/1.1 200 OK (application/pdf)
19	3683 119.921382	::1	::1	HTTP	398	GET /ANZ1.inp HTTP/1.1

For the anz-logo.jpg look after the response of that specific request (line #140) and copy its code as a HEX stream

Screenshot of NetworkMiner tool showing the HTTP traffic. The packet list shows various requests and responses. The details pane highlights the response for line 140, which is a GET request for /anz-logo.jpg. The hex and ASCII panes show the raw data of the response, which is a JPEG image.

The right-click context menu for the selected packet (Line 140) includes options like "Copy", "Copy Bytes as Hex + ASCII Dump", "Copy Bytes as Hex Stream", and "Copy Bytes as Raw Binary".

The bottom status bar indicates the total number of packets: 3683.

I paste the copied Hex in HxD HEX editor

HxD - [Sin título4]

Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda

Sin título4

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Texto decodificado

000012C0 DD 73 19 F3 B0 7D 55 89 F1 59 3E 5A AC F9 5A 3F Ys.ó?UññY>Z-nú?

000012D0 D3 78 8F CA 83 F5 78 D6 A4 AE 71 5C 46 A9 E5 Ox.ÉfóxñmEq(Fj@á

000012E0 A9 9D DA F3 4C ED 67 BA C0 5C D0 01 60 36 00 00 @.ÓÚLlg@Ó.'6..

000012F0 1D CA D6 EB A6 B1 A8 72 DA 77 3B 49 0A 28 55 12 .ÉOe;#rUw;I.(U.

00001300 42 8A 10 49 05 5D 08 84 4A 10 52 55 4D 09 21 45 B5.I.].J.RUM.!E

00001310 34 24 84 43 42 57 42 80 42 10 8A 12 4D 08 12 13 4C.CBWBBB.Ş.M...

00001320 42 04 84 D0 81 21 34 20 10 84 20 61 09 21 10 D0 B..B.!4 ..a.!.D

00001330 84 20 10 92 15 53 42 48 40 D0 92 13 68 0A 12 42 ..'..SBH@B'.h..B

00001340 8A 68 49 08 1A 12 42 01 08 42 06 84 90 81 A1 24 ŠhI...B...B...;S

00001350 22 84 21 08 04 21 08 1A 12 42 06 84 90 81 A4 84 "„!..!...B...M"

00001360 22 04 D2 42 06 84 90 81 A1 24 20 68 49 0A 81 08 ".OB...;S.h!...

00001370 42 80 42 10 80 42 10 80 42 48 40 D0 84 BCB.EB.EBH@B"

00001380 22 84 21 08 04 21 08 04 90 84 0C 21 08 "„!..!...!...!..!

00001390 44 08 42 10 08 42 10 08 42 10 7F FF D9 D.B..B..B..yÜ

Desplazamiento(h): 13A0 * Modificado * Sobreescribir

Editoras especiales Inspector de datos

Binary (8 bit) Inválido

Int8 lr;a: Inválido

UInt8 lr;a: Inválido

Int16 lr;a: Inválido

UInt16 lr;a: Inválido

Int24 lr;a: Inválido

UInt24 lr;a: Inválido

Int32 lr;a: Inválido

UInt32 lr;a: Inválido

Int64 lr;a: Inválido

UInt64 lr;a: Inválido

LEB128 lr;a: Inválido

ULEB128 lr;a: Inválido

AnsiChar / char8_t Inválido

WideChar / char16_t Inválido

Punto de código UTF-8 Inválido

Orden de bytes Little endian Big endian

Base hexadecimal (para números enteros)

And then save the file as anz-logo.jpg obtaining this way the following image file

HxD - [Sin título5]

Archivo Edición Buscar Ver Análisis Extras Ventanas Ayuda

Sin título5

Offset(h) 00 01 02 03 04 05 06 07 08

00001200 A2 7C 95 D8 2E BC 6F 0C AE

00001210 73 5E C7 16 B9 AE 1B 08 23

00001220 1B 43 3C 65 92 5B E1 4B 4F

00001230 F1 CC CE E0 A6 88 D4 BB

00001240 19 FF 00 60 5A AF E0 FF 00

00001250 6A CB 49 DF AB 1C 4C 84

00001260 7C 52 B6 09 29 A7 9A 3F 05

00001270 0C ED 71 BB 25 6B 3A 71

00001280 D6 DE FF 00 08 59 24 4D 90

00001290 E8 52 31 CF AE 89 5D 0F 6D

000012A0 6B CE C1 F5 56 23 DD 73 1A

000012B0 CC FE 5A BD 1E 85 E7 0F 75

000012C0 DD 73 19 F3 B0 7D 55 89 F1

000012D0 D3 78 8F CA 83 F5 78 D6 A4

000012E0 A9 9D DA F3 4C ED 67 BA C0

000012F0 1D CA D6 EB A6 B1 A8 72 DA

00001300 42 8A 10 49 09 5D 08 84 4A

00001310 34 24 84 43 42 57 42 80 42

00001320 42 04 84 D0 81 21 34 20 10

00001330 84 20 10 92 15 53 42 48 40

00001340 8A 68 49 08 1A 12 42 01 08

00001350 22 84 21 08 04 21 08 1A 12

00001360 22 04 D2 42 06 84 90 81 A1

00001370 42 80 42 10 80 42 10 80 42

00001380 22 84 21 08 04 21 08 04 21

00001390 44 08 42 10 08 42 10 08 42

Desplazamiento(h): 13A0

Guardar como

Nombre: anz-logo.jpg

Tipo: Todos los archivos (*.*)

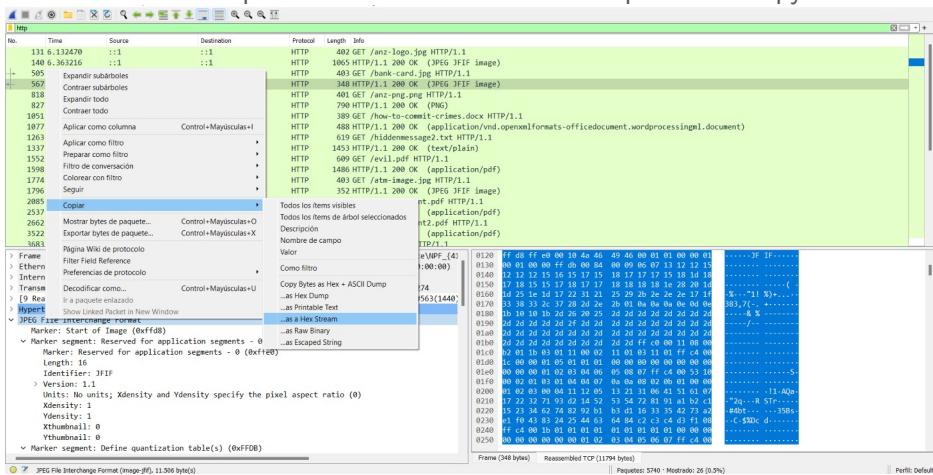
Ocultar carpetas Guardar Cancelar

Escritorio Descargas Documentos Imágenes Música

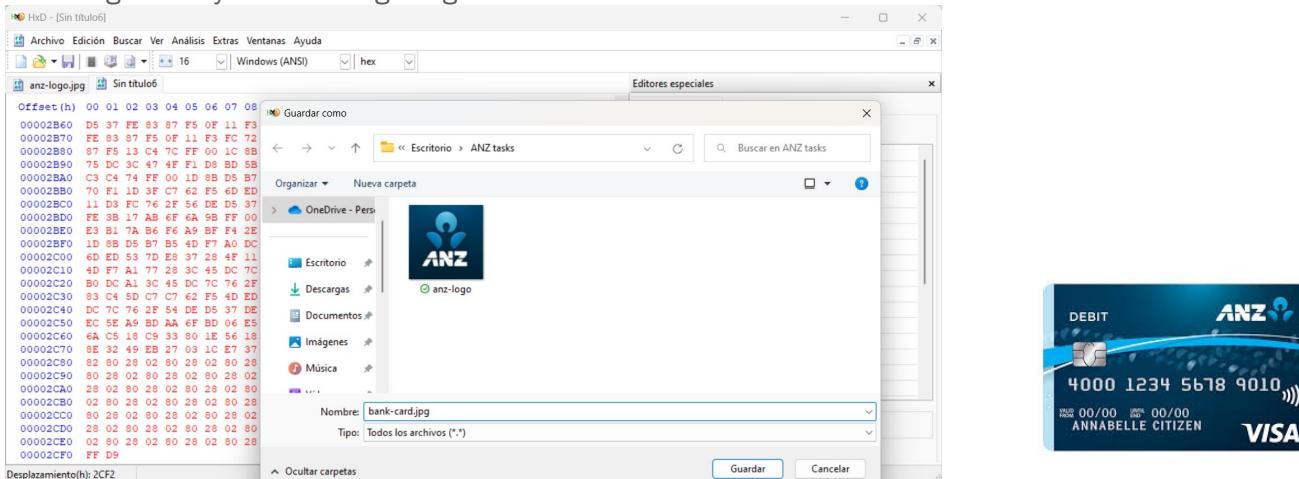
Ningún elemento coincide con el criterio de búsqueda.

For the bank-card.jpg image the same steps must be followed

First search the response to the bank-card GET request and copy the file code as a Hex Stream



Paste the copied Hex in HxD HEX editor and then save the file as anz-logo.jpg obtaining this way the following image file

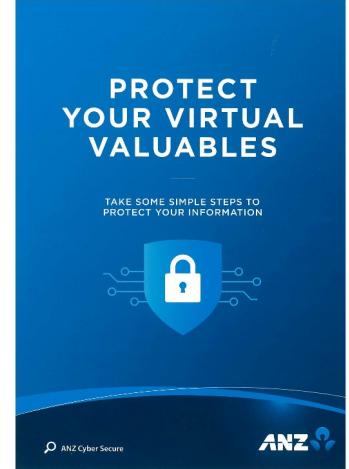
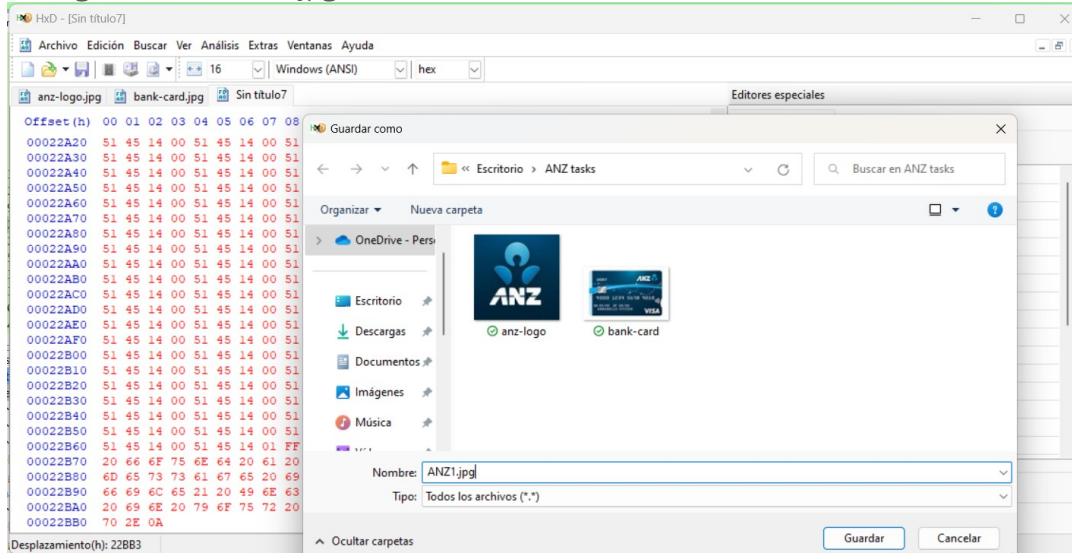


Sub-task 2:

- The network traffic for the images "ANZ1.jpg" and "ANZ2.jpg" is more than it appears.
- Extract the images, include them and mention what is different about them in your report.

Following the same steps explained in the Sub-task 1, copy the files as a Hex Stream and save the files in the HxD Hex editor and obtain the images

Saving the file as ANZ1.jpg with the HxD Hex editor.



Copying the file code as a Hex Stream with Wireshark.

MAKE A 'PACT'
TO PROTECT YOUR VIRTUAL VALUABLES

CALL OUT
before sharing your personal information

Ask yourself: do I really need to give my information to this website or this person? If I do, consider first right, don't share it.

ACTIVATE
two layers of security with two-factor authentication

Use two-factor authentication for an extra layer of security to keep your personal information safe.

REPORT
Report suspicious messages from ANZ:

Email: hscs@cybersecurity.anz.com
Report fraudulent or unusual ANZ account activity:

137.228 / +61 3 8693 7113 (Corporate/Business Client)
133.350 / +61 3 9663 8833 (Personal Banking Customers)

Australia and New Zealand Banking Group Limited ABN 11 001 011 131 AFSL 239308 ACN 000 121 131

Differences between files:

We can notice a few differences between files such as the file size expressed at the “File Data” field among others.

- ✓ Hypertext Transfer Protocol
 - > HTTP/1.1 200 OK\r\nDate: Fri, 16 Aug 2019 00:49:42 GMT\r\nServer: Apache/2.4.6 (CentOS)\r\nLast-Modified: Thu, 15 Aug 2019 14:16:05 GMT\r\nETag: "2bd8e-5902883a60136"\r\nAccept-Ranges: bytes\r\nContent-Length: 179598\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: image/jpeg\r\n\r\n[HTTP response 1/1]
[Time since request: 2.704316000 seconds]
[\[Request in frame: 4074\]](#)
[Request URI: http://localhost:8000/ANZ2.jpg]
File Data: 179598 bytes
- ✓ Hypertext Transfer Protocol
 - > HTTP/1.1 200 OK\r\nDate: Fri, 16 Aug 2019 00:49:30 GMT\r\nServer: Apache/2.4.6 (CentOS)\r\nLast-Modified: Thu, 15 Aug 2019 14:14:04 GMT\r\nETag: "22bb3-590287c71be98"\r\nAccept-Ranges: bytes\r\nContent-Length: 142259\r\nKeep-Alive: timeout=5, max=100\r\nConnection: Keep-Alive\r\nContent-Type: image/jpeg\r\n\r\n[HTTP response 1/1]
[Time since request: 3.052568000 seconds]
[\[Request in frame: 3683\]](#)
[Request URI: http://localhost:8000/ANZ1.jpg]
File Data: 142259 bytes
- > JPEG File Interchange Format

Both ANZ1.jpg and ANZ2.jpg have hidden messages that we can observe in the HxD Hex editor at the bottom of their decoded text.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
00022B00	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B10	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B20	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B30	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B40	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B50	51 45 14 00 51 45 14 00 51 45 14 00 51 45 14 00	QE..QE..QE..QE..
00022B60	51 45 14 00 51 45 14 01 FF D9 59 6F 75 27 76 65	QE..QE..ÿYou've
00022B70	20 66 6F 75 6E 64 20 61 20 68 69 64 64 65 6E 20	found a hidden
00022B80	6D 65 73 73 61 67 65 20 69 6E 20 74 68 69 73 20	message in this
00022B90	66 69 6C 65 21 20 49 6E 63 6C 75 64 65 20 69 74	file! Include it
00022BA0	20 69 6E 20 79 6F 75 72 20 77 72 69 74 65 20 75	in your write u
00022BB0	70 2E 0A	p..

ANZ1 message :“You’ve found a hidden message in this file! Include it in your write”

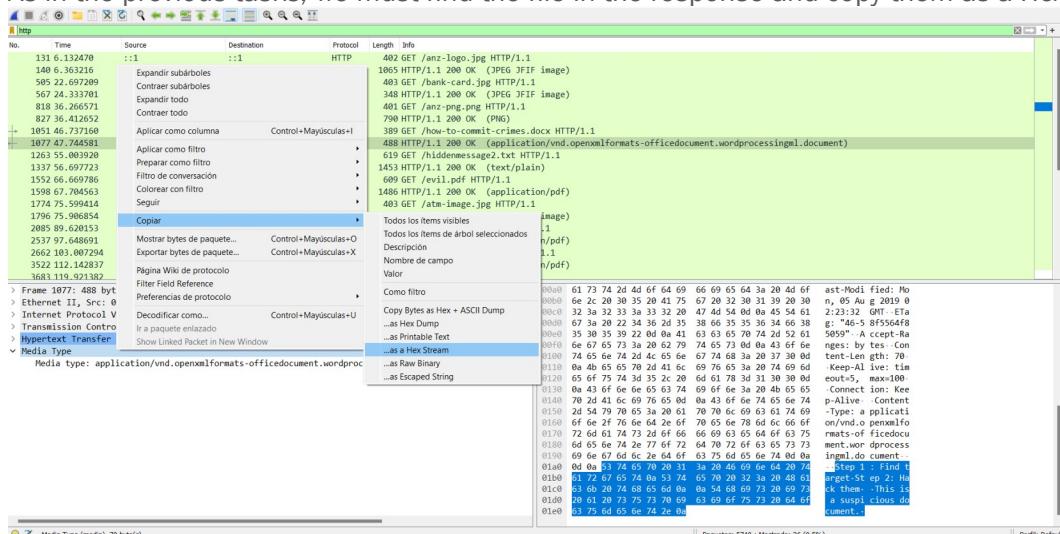
Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
0002BD00	51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14	QE..QE..QE..QE..
0002BD10	51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14	QE..QE..QE..QE..
0002BD20	51 40 05 14 51 40 05 14 51 40 05 14 51 40 05 14	QE..QE..QE..QE..
0002BD30	51 40 05 14 51 40 05 14 51 40 05 14 51 40 1F FF	QE..QE..QE..QE..ÿ
0002BD40	D9 59 6F 75 27 76 65 20 66 6F 75 6E 64 20 74 68	ÿYou've found th
0002BD50	65 20 68 69 64 64 65 6E 20 6D 65 73 73 61 67 65	e hidden message
0002BD60	21 0A 49 6D 61 67 65 73 20 61 72 65 20 73 6F 6D	!.Images are som
0002BD70	65 74 69 6D 65 73 20 6D 6F 72 65 20 74 68 61 6E	etimes more than
0002BD80	20 74 68 65 79 20 61 70 70 65 61 72 2E 0A	they appear..

ANZ2 message: “You’ve found the hidden message!. Images are sometimes more than they appear.”

Sub-task 3:

- The user downloaded a suspicious document called "how-to-commit-crimes.docx"
- Find the contents of this file and include it in your report.

As in the previous tasks, we must find the file in the response and copy them as a Hex stream.



We can already see the text in the “decoded text” of the HxD HEX editor or open the file that just saved with any docx reader.

Offset (h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
00000000	53 74 65 70 20 31 3A 20 46 69 6E 64 20 74 61 72	Step 1: Find tar
00000010	67 65 74 0A 53 74 65 70 20 32 3A 20 48 61 63 6B	get. Step 2: Hack
00000020	20 74 68 65 6D 0A 0A 54 68 69 73 20 69 73 20 61	them..This is a
00000030	20 73 75 73 70 69 63 69 6F 75 73 20 64 6F 63 75	suspicious docu
00000040	6D 65 6E 74 2E 0A	ment...[]

Decoded text:

Step 1: Find target

Step 2: Hack them

This is a suspicious document.

Sub-task 4:

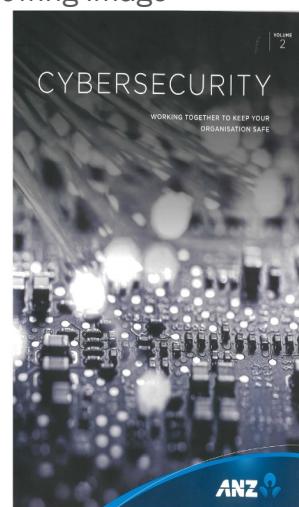
- The user accessed 3 pdf documents: ANZ_Document.pdf, ANZ_Document2.pdf, evil.pdf
- Extract and view these documents. Include images of them in your report.

As in the previous tasks, copy as HEX stream the code of the file from response to the specific GET request

NetworkMiner Screenshot showing the context menu for Frame 1284 (HTTP/1.1 200 OK). The menu path 'Copiar' is highlighted. The right pane displays the raw hex and ASCII data for the PDF file.

Copy that code in the HxD Hex editor and save the file as pdf obtaining the following image

HxD Hex Editor Screenshot showing the raw hex dump of the copied PDF data. An 'Guardar como' (Save As) dialog box is open, showing the file name 'ANZ_Document.pdf' and the file type 'Todos los archivos (*.*)'. The file is being saved to the 'Escritorio' (Desktop) folder.

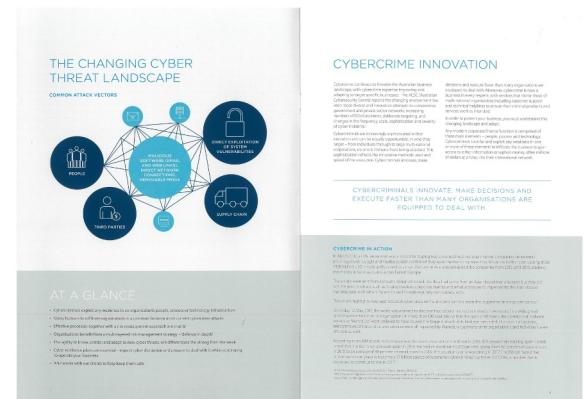


Repeat with the “ANZ_Document2.pdf” file

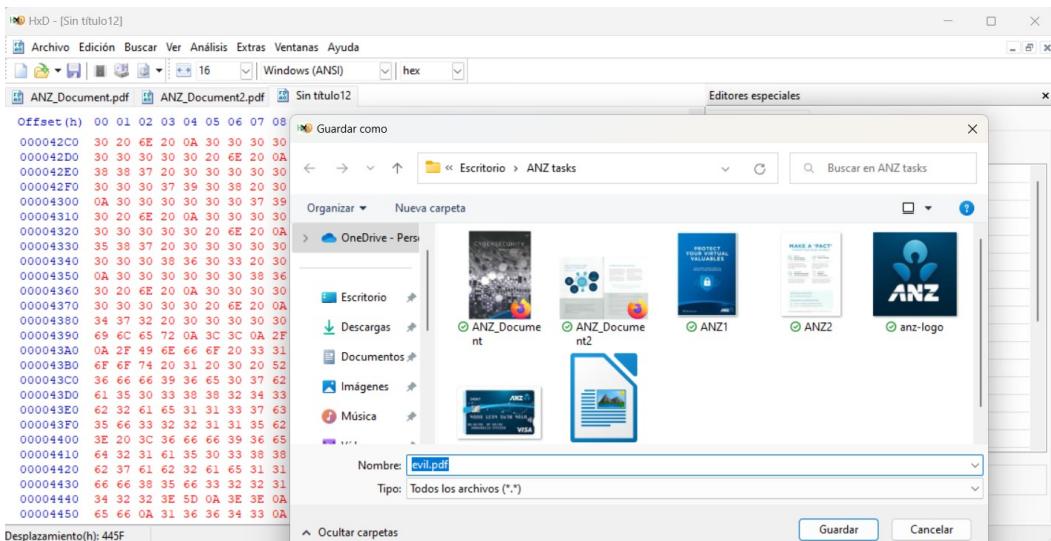
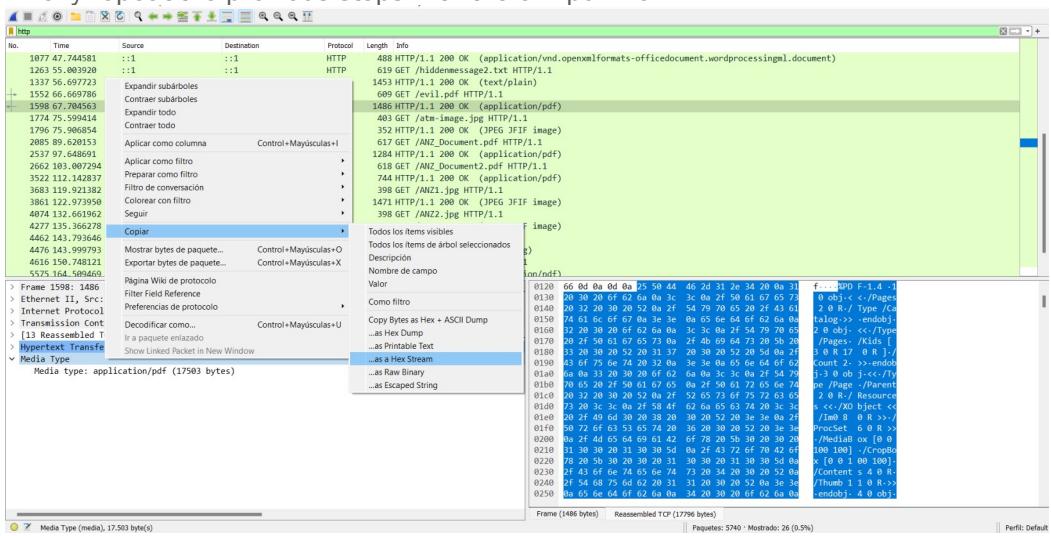
No. Time Source Destination Protocol Length Info

1263	55.003920	::1	::1	HTTP	619	GET /hiddenmessage2.txt HTTP/1.1
1337	56.697723	::1	::1	HTTP	1453	HTTP/1.1 200 OK (text/plain)
1552	66.66977	-	-	HTTP	609	GET /evil.pdf HTTP/1.1
1598	67.7045	Expander subáboles	-	HTTP	1486	HTTP/1.1 200 OK (application/pdf)
1774	75.5984	Contraria subáboles	-	HTTP	483	GET /atm-image.jpg HTTP/1.1
1786	76.59848	Expandir todo	-	HTTP	357	HTTP/1.1 200 OK (JPEG/JFIF image)
2085	89.6201	Contraria todo	-	HTTP	617	GET /ANZ/Document2.pdf HTTP/1.1
2537	97.6486	-	-	HTTP	1264	HTTP/1.1 200 OK (application/pdf)
2662	103.007	Aplicar como columna	-	Control+Mayúsculas+I	618	GET /ANZ/Document2.pdf HTTP/1.1
3522	112.1342	Aplicar como filtro	-	Control+Mayúsculas+I	744	HTTP/1.1 200 OK (application/pdf)
3683	119.921	Preparar como filtro	-	Control+Mayúsculas+I	398	GET /ANZ1.jpg HTTP/1.1
3861	122.973	Filtro de conversación	-	Control+Mayúsculas+I	1471	HTTP/1.1 200 OK (JPEG/JFIF image)
4074	132.661	Colorar con filtro	-	Control+Mayúsculas+I	398	GET /ANZ2.jpg HTTP/1.1
4277	135.366	Seguir	-	Control+Mayúsculas+I	282	HTTP/1.1 200 OK (JPEG/JFIF image)
4462	143.793	-	-	Control+Mayúsculas+I	284	HTTP/1.1 200 OK (JPEG/JFIF image)
4476	143.999	Copiar	-	Control+Mayúsculas+I	284	HTTP/1.1 200 OK (JPEG/JFIF image)
4616	158.748	Mostrar bytes de paquete...	-	Control+Mayúsculas+I	Todos los items visibles	
5575	164.509	Exportar bytes de paquete...	-	Control+Mayúsculas+X	Todos los items del árbol seleccionados	
>	Página Wiki de protocolo	-	-	Descripción		
>	Ethernet II, ...	-	-	Nombre de campo		
>	Internet Prot...	-	-	Valor		
>	Transmission (...	-	-	Como filtro		
[618 Reassembl...	Decodificar como...	-	-	Copy Bytes as Hex + ASCII Dump		
Hypertext Trai...	Ir a paquete enlazado	-	-	...as Hex Dump		
Media Type	Show Linked Packet in New Window	-	-	...as Printable Text		
	Media type: application/pdf (843159 bytes)	-	-	...as a Hex Stream		
		-	-	...as Raw Binary		
		-	-	...as Escaped String		

Copy that code in the HxD Hex editor and save the file as pdf obtaining the following file:



Finally repeat the previous steps with the evil.pdf file.



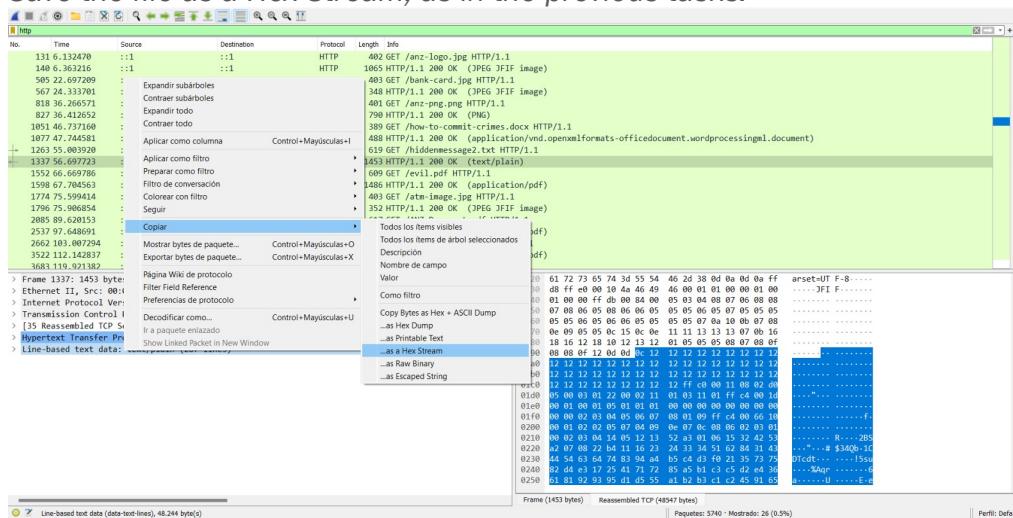
We obtain a 2 pages pdf file that in the first one has a completely blue page and in the second one has the following message:

More suspicious stuff good job!

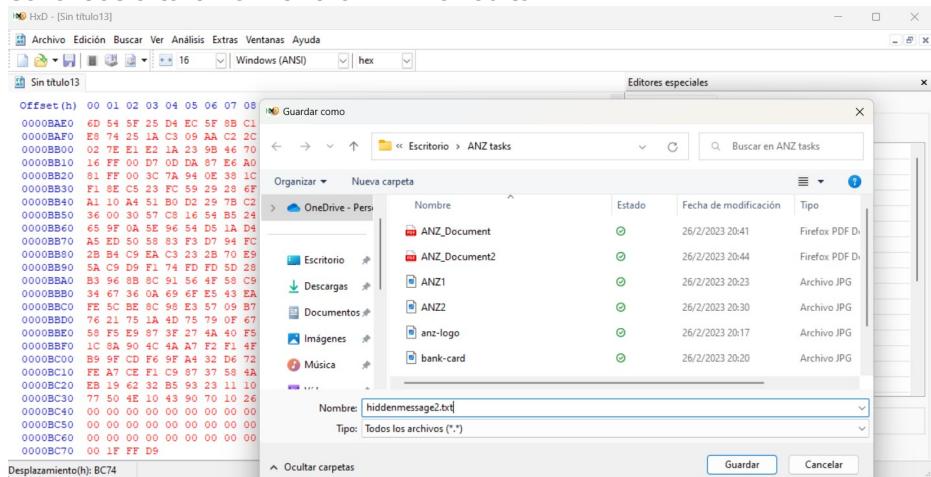
Sub-task 5:

- The user also accessed a file called "hiddenmessage2.txt"
- What is the contents of this file? Include it in your report

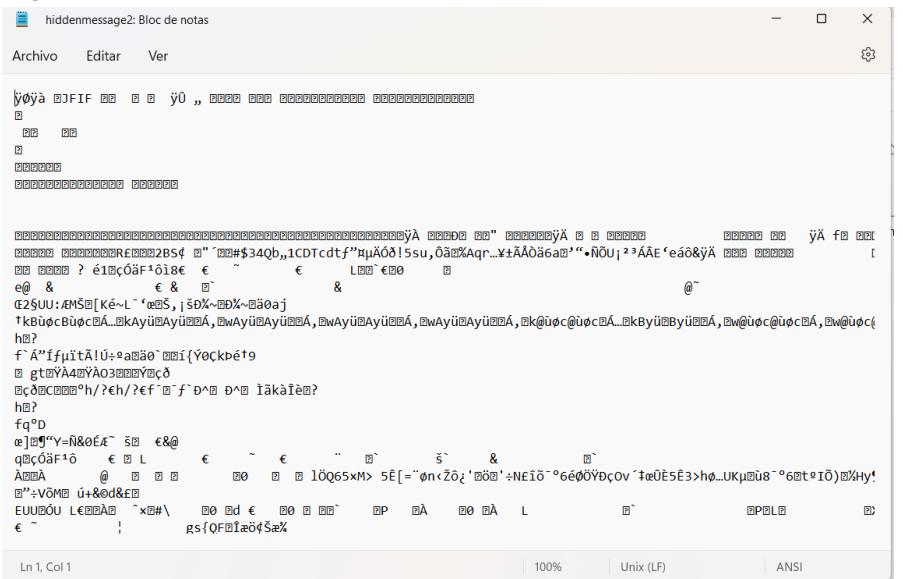
Save the file as a Hex Stream, as in the previous tasks.



Save it as a text file with the HxD Hex editor



When opening we can notice that the text is impossible to read, but we can see the signature of the JFIF file.



```
FFD8 hidddenmessage2: Bloc de notas
Archivo Editar Ver
FFD8 FF 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a ff
0130 d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00
0140 01 00 00 ff db 00 84 00 05 03 04 08 07 06 08 08
0150 07 08 06 05 08 06 06 05 05 05 06 05 07 05 05 05
0160 05 05 06 05 06 06 05 05 05 05 07 0a 10 0b 07 08
0170 0e 09 05 05 0c 15 0c 0e 11 11 13 13 13 07 0b 16
0180 10 15 12 12 12 12 12 01 05 05 05 07 09 05 05 05
```

FF D8 is the file signature for jpg images, so I save it as jpg.

0120	61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a ff	arset=UT F-8.....
0130	d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00JFI F.....
0140	01 00 00 ff db 00 84 00 05 03 04 08 07 06 08 08
0150	07 08 06 05 08 06 06 05 05 05 06 05 07 05 05 05
0160	05 05 06 05 06 06 05 05 05 05 07 0a 10 0b 07 08
0170	0e 09 05 05 0c 15 0c 0e 11 11 13 13 13 07 0b 16
0180	10 15 12 12 12 12 12 01 05 05 05 07 09 05 05 05

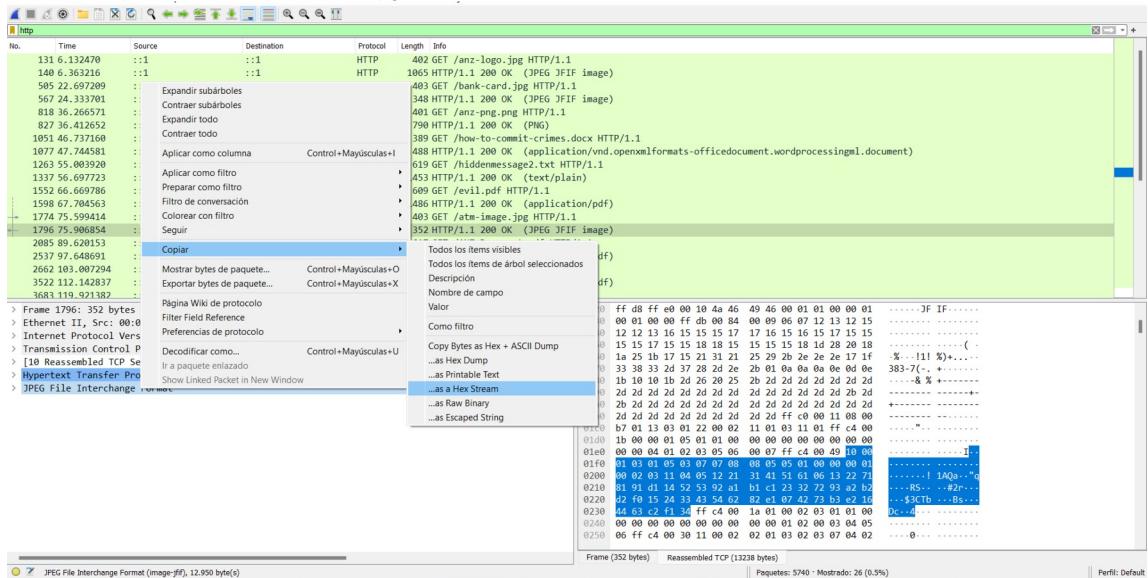
Saved as jpg we can see the following image.



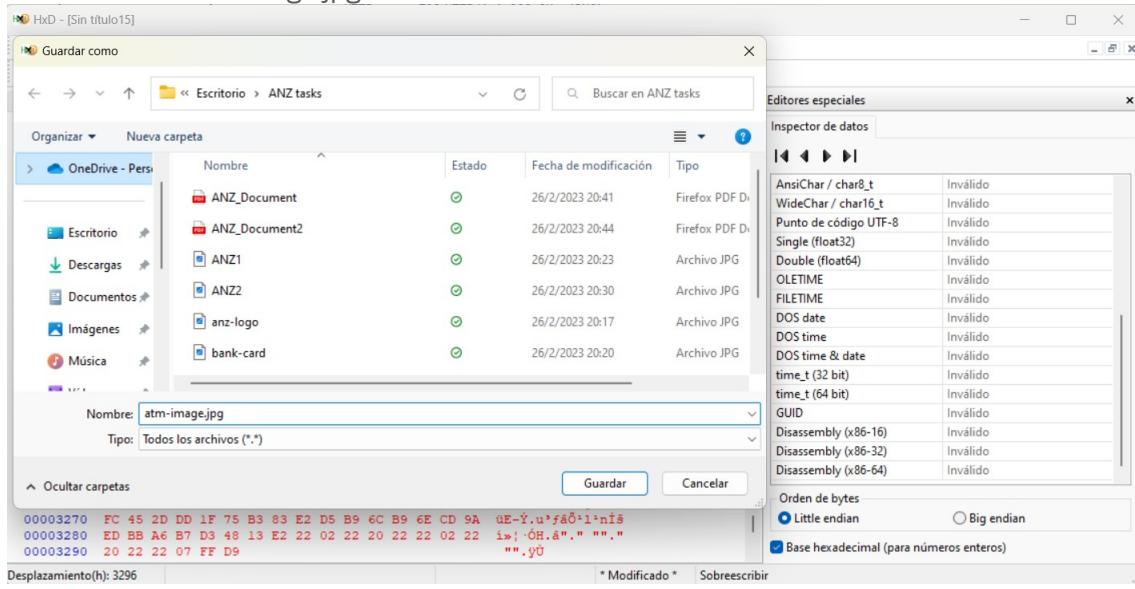
Sub-task 6:

- The user accessed an image called "atm-image.jpg"
- Identify what is different about this traffic and include everything in your report.

As in the previous tasks we copy the file code as a Hex stream.



And save it as atm-image.jpg



Obtaining the following image.



But wait, there is more!

There is a hidden image embedded in the amt-image.jpg file. That could be noticed when inspecting the file stream with Wireshark. In the image below, I identify the embedded jpg image by its JFIF signature, so I copied its hex code and saved it to a new file called "embedded.jpg" getting the following image of a thief.

atm-image.jpg

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
00001E60	8C 02 BA 8B 86 E4 E5 02 23 45 35 D1 3F 0A 6D 12	E.º<+ä. #E5Ñ?.m.
00001E70	83 45 00 2A 6B 9A A4 19 AE 21 40 91 55 2A 76 04	fE.*kñ. @!@'U'v.
00001E80	8A 10 C4 31 4E D7 2E 5C A8 43 96 10 82 23 C5 DC	Š.ÄINx. \^C-, #ÄÜ
00001E90	81 32 ED 5C B9 05 D4 69 74 42 19 13 0A E5 C9 C4	.2i\^, .ÖtB.., ÄÉA
00001EA0	35 3C 90 B6 67 80 AE E5 9D 93 09 6B 86 84 AE 5C	5k. Ig@ä. ", kt. @\
00001EB0	A9 E9 33 47 5C 66 79 8C 52 96 8A E5 A7 1C BD 8B	@é3GfyCR-ŠåS. +k
00001EC0	97 2D 28 CC 28 6A 92 20 B9 72 20 25 C2 A5 60 48	--(í(j ^ %Ä" H
00001ED0	B9 10 13 34 28 1C E1 53 99 5C B9 40 0E 1D AB 85	^...4(.äSM^@..<..
00001EE0	12 2E 50 82 87 22 8B 8D 34 A9 5C B9 42 33 98 0E	..P, ^<.4@. ^B3".
00001EF0	DC 94 AC 62 45 C8 80 7B B2 A3 B7 7C 77 AE 96 D0	Ü~bEEE{^E: w@-D
00001F00	5B 95 41 35 22 94 35 00 68 49 D3 FF 00 8B 97 20	[A5"5.hIOy.<-
00001F10	42 27 DB 0E E0 A4 B2 BB 2A 6E F7 6C 48 B9 40 A2	B'Ü.ä#^x*x-n=1H:@c
00001F20	7A 25 09 17 22 11 1C 07 F7 4D C5 EC 5C B9 00 8A	z%."...+Mai\^..S
00001F30	D7 AE 24 AE 5C A1 0E 0E 29 CD 90 15 CB 94 20 B5	*@S@V;(..)I.E" p
00001F40	5C B9 72 84 3F FF D9 FF D8 FF E0 00 10 4A 46 49	\r.,?yÜ@yä..JFT
00001F50	46 00 01 01 00 00 01 00 01 00 00 FF DB 00 94 00	F.....yÜ..
00001F60	09 06 07 12 13 12 15 12 12 16 15 15 18 17
00001F70	17 15 16 15 15 15 16 16 18 1B 17 15 16 17 17 19
00001F80	15 13 18 1E 2A 22 18 1F 26 1B 16 15 21 31 21 26%"..&..!1!&
00001F90	29 2B 2E 2E 2F 18 1F 33 38 33 2C 37 28 2D 2E 2B)+. /..383, 7(-.+
00001FA0	01 0A 0A 0A 0D 0D 0E 15 0F 10 17 2B 19 17 19 2D+....
00001FB0	2B 2B 37 2B 2D 2B 2D 2B 37 2B 2D 38 2D 2B	++7+-+--+7+-+8+-
00001FC0	30 37 38 2E 2D 2D 38 2D 2B 2D 37 2B 2B 37	078.--8---+7+++7
00001FD0	2D 2B 37 2B 2B 2B 2B 2D 37 2B 2B 2B 37	=+7+++++--+7-7+++

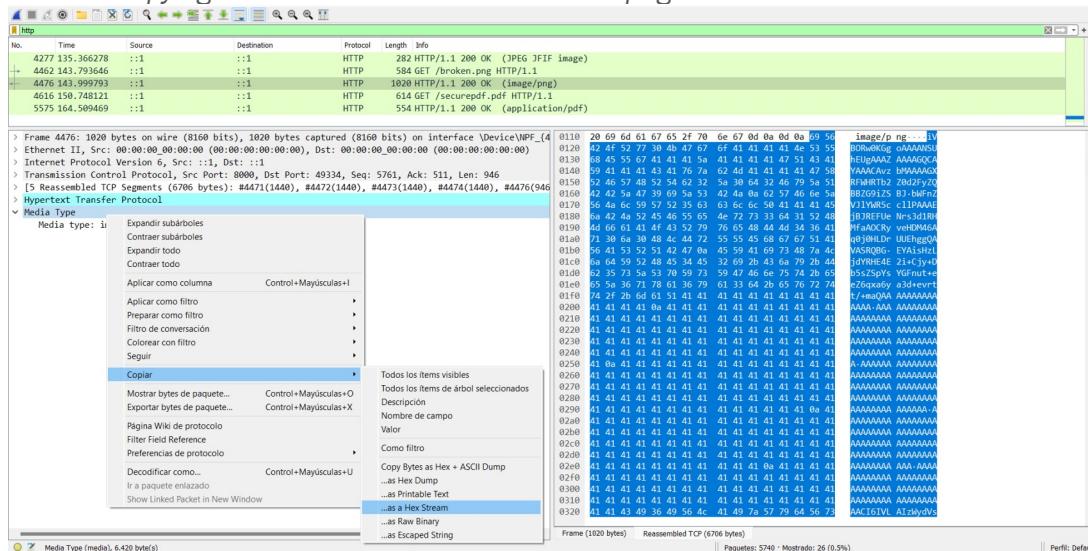


shutterstock.com • 567329461

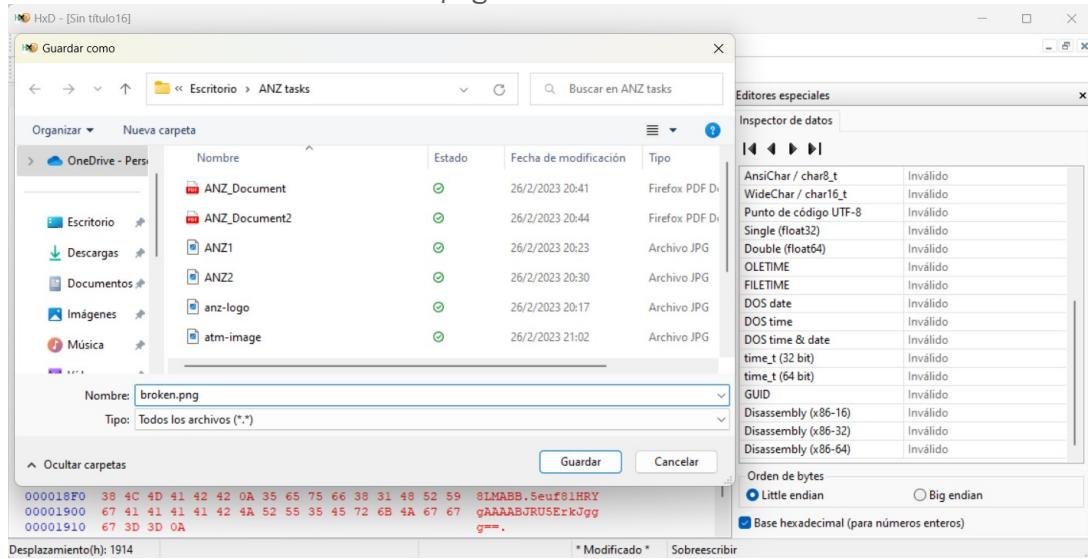
Sub-task 7:

- The network traffic shows that the user accessed the image "broken.png"
- Extract and include the image in your report.

I started copying as a HEX stream the code of the png file.



Saved it in the HxD Hex editor as a png file.



I couldn't open the file or identify the file signature, so I tried to investigate if the file was encrypted. As we can see with the online decoder <https://www.base64decode.org/> the broken.png file is encoded in Base64 and once decoded we can already read some information about it. We can also go to the terminal and type:
`$cat broken.png | base64-d | xxd` thus getting the decoded hex dump.

Simply enter your data then push the decode button.

Now that we know the file is Base64 encoded, we can go to the terminal and redirect the contents of broken.png to a new file or use online tools like <https://base64.guru/converter/decode/image/png> to decode and get the png image.

Base64 to PNG

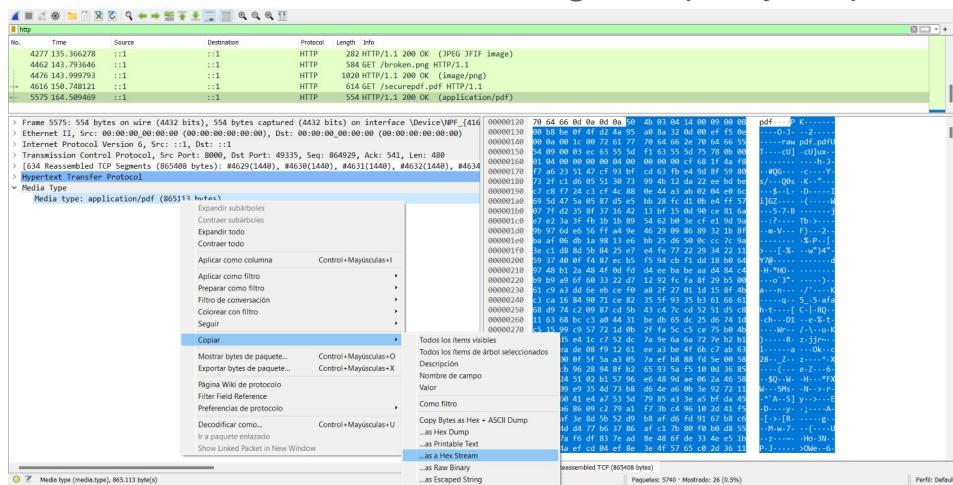
Convert Base64 to PNG online using a free decoding tool that allows you to decode Base64 as PNG image and preview it directly in the browser. By and large, the "Base64 to PNG" converter is similar to [Base64 to Image](#), except that it this one forces the MIME type to be "image/png". If you are looking for the reverse process, check [PNG to Base64](#).

Decode Base64 to PNG

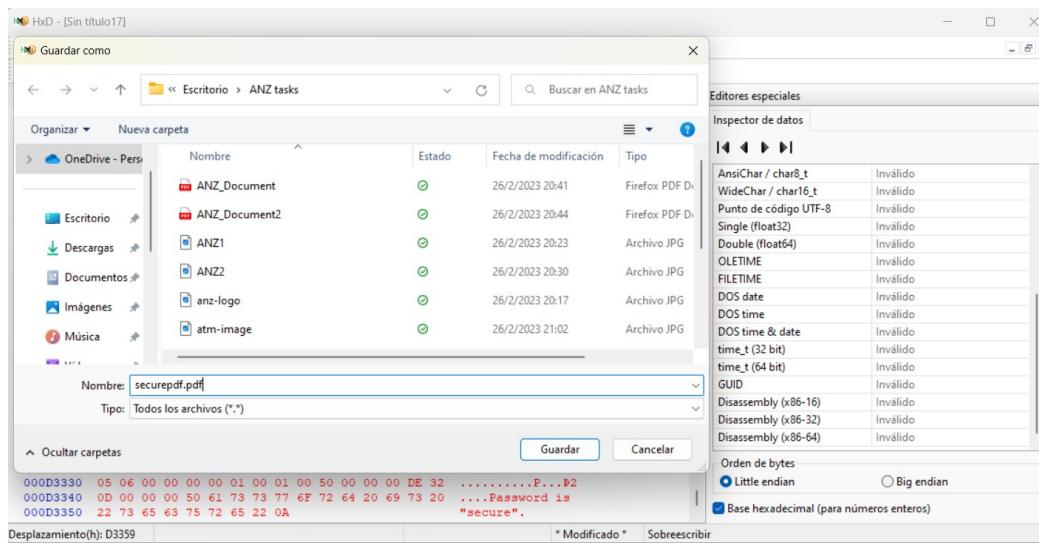
[Preview PNG Image](#) | [Toggle Background Color](#)

Sub-task 8:

- The user accessed one more document called **securepdf.pdf**
- Access this document include an image of the pdf in your report. Detail the steps to access it.



I tried to save it as a pdf file first as in the previous tasks but it wasn't working.



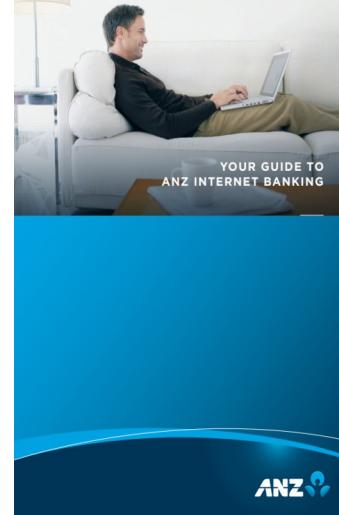
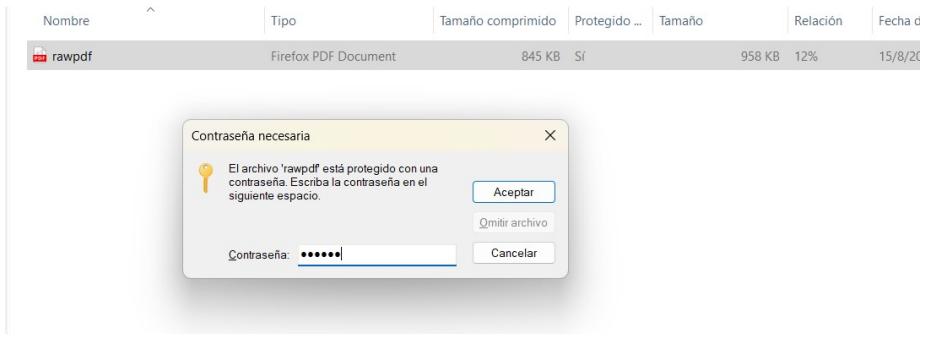
Then I noticed that the file signature (50 4B 03 04) indicates that it was a zip file instead of a pdf. So I save it as securepdf.zip

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
00000000	F0 4B 03 04 14 00 09 00 08 00 B8 BE 0F 4F D2 4A	EK.....,%.OÖJ
00000010	95 A0 8A 32 0D 00 EF F5 0E 00 0A 00 1C 00 72 61	• Š2..iö.....ra
00000020	77 70 64 66 2E 70 64 66 55 54 09 00 03 EC 63 55	wpdf.pdfUT...icU
00000030	5D F1 63 55 5D 75 78 0B 00 01 04 00 00 00 00 04	jñcUjux.....
00000040	00 00 00 00 CF 68 1F 4A F8 F7 A6 23 51 47 CF 93ih.Js+;#QGÍ"
00000050	BF CD 63 FB E4 9D 8F 59 80 73 2F C1 D6 05 51 30	žícuä..Yës/AÖ.Q0
00000060	73 99 4B 12 DA 22 EE BD BE C7 C8 F7 24 C3 CF 4C	s"K.Ú"iñçÉ-äÄL
00000070	88 0E 44 A3 AB 02 04 E0 6C 69 5D 47 5A 05 87 D5	^.Df«.äli]GZ.‡Ö
00000080	E5 BB 28 FC D1 0B E4 FF 57 07 7F D2 35 8F 37 16	å»(üN.äyw..ö5.7.
00000090	42 13 BF 15 0D 90 CE 81 6A E7 E2 3A 3F FB 1B 1B	B.¿...i.jçä:žö..
000000A0	89 54 62 20 3E CF E1 9D 9A 9B 97 6D E6 56 FF A4	#Tb>íá.š>-mæVý¤
000000B0	9E 46 29 09 86 89 32 1B 8F BA AF 06 DB 1A 98 13	žF).tñ2..-Ü.~.
000000C0	E6 BB 25 D6 50 0C CC 7C 9A 3E C1 D8 8D 5B 84 25	æ»%ÖP.í š>Á0. [..%
000000D0	E7 E4 FE 77 22 29 34 22 11 59 37 40 0F F4 87 EC	çäpw")4",Y7@.ö‡í
000000E0	B5 F5 94 CB F1 DD 18 B0 64 97 48 B1 2A 48 4F OD	uö"ÉñY."d-H‡*HO.
000000F0	FD D4 EE BA AA D4 84 C4 B9 B9 A9 6F 60 33 22	ýôi¤äÖ,Ä¹:Øo'3"
00000100	D7 12 92 FC FA 8F 29 B5 00 61 C9 A3 DD 6E EB CE	*.'üü.)p.aÆzÍnëí
00000110	F0 A8 2F 27 01 1D 15 8F 4B C3 CA 16 84 90 71 CE	ö"/'....KÄ...qí
00000120	82 35 5F 93 35 B3 61 66 61 68 D9 74 C2 09 87 CD	,5."5"afahÜtA.‡í
00000130	5B 43 C4 7C CD 52 51 D5 C8 11 63 68 BC C3 A0 44	[CA]íRQÖE.ch‡Ä D
00000140	31 BE DB 65 DC 25 D6 74 1D C5 15 99 C9 57 72 1D	lñüÜ%öt.Ä.¶éWr.
00000150	OB 2F FA 5C C5 CE 75 B0 4B 29 CA D5 E4 1C C7 52	./úÅfuºK)Éða.ÇR
00000160	DC 7A 9E 6A 6A 72 7E B2 B1 6C B6 EA DE 08 F9 12	Üzžjjr~"‡l¶éþ.ù.
00000170	61 EE A3 BE 4F 6B C7 AB 63 32 38 00 0F 5F 5A A3	aï§%OkÇ«c28.._ZŁ
00000180	05 7A EF B8 88 FD 5E 00 58 E7 F7 CB 96 28 94 8F	.zi,^y^.Xç-È-(".
00000190	B2 65 93 5A F5 10 0D 36 85 80 8E 24 51 02 B1 57	“e”ZŁ..6..€Ž\$Q.‡W

At the end of the decoded text we can see that the password to open the content in the zip folder is “secure”, so we proceed to open the file.

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Texto decodificado
000D32F0	95 A0 8A 32 0D 00 EF F5 0E 00 0A 00 18 00 00 00	• Š2..iö.....
000D3300	00 00 00 00 00 00 A4 81 00 00 00 00 72 61 77 70ñ.....rawp
000D3310	64 66 2E 70 64 66 55 54 05 00 03 EC 63 55 5D 75	df.pdfUT...icUju
000D3320	78 0B 00 01 04 00 00 00 00 04 00 00 00 00 50 4B	x.....PK
000D3330	05 06 00 00 00 00 01 00 01 00 50 00 00 00 DE 32P...Þ2
000D3340	0D 00 00 00 50 61 73 73 77 6F 72 64 20 69 73 20Password is
000D3350	22 73 65 63 75 72 65 22 0A	"secure".

With the “secure” password we can open the following pdf file



Links used for the resolution:

https://en.wikipedia.org/wiki/List_of_file_signatures

<https://www.base64decode.org/>

<https://base64.guru/converter/decode/image/png>

Sub-task 7 commands explained:

\$cat broken.png | base64 -d | xxd

cat : Concatenates FILE(s), or standard input, to standard output.

Base64 -d : Decodes the Base64 code.

Xxd : creates a hex dump of a given file or standard input.