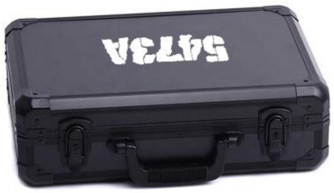
NeverLAN CTF 2021: Stego – suspicious briefcase by g0dd42d (Not The PPP)

Challenge (20pts):

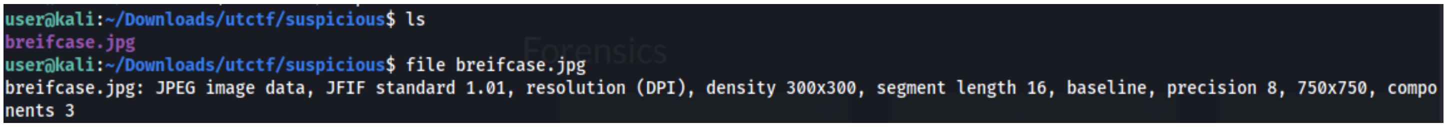
We are given this text and image attachment:

“we found this briefcase... something doesnt seem right about it”



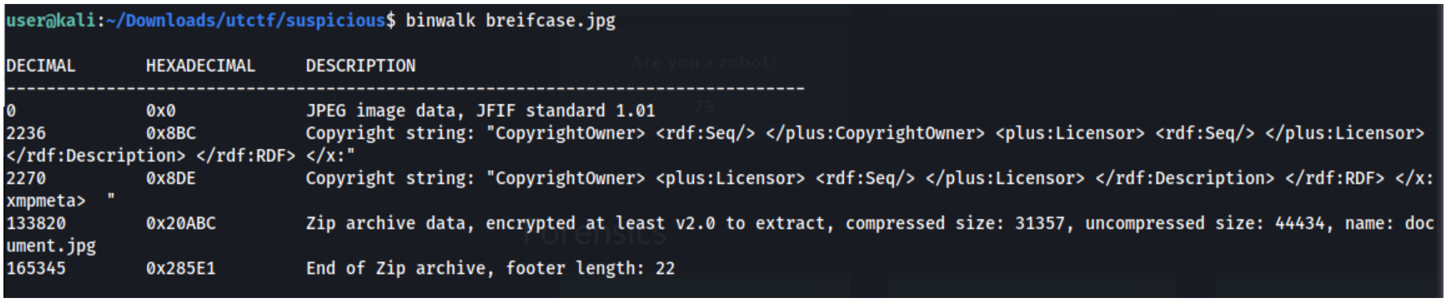
briefcase.jpg

Yes, briefcase is misspelled on the challenge.



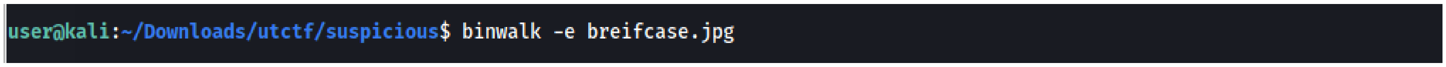
```
user@kali:~/Downloads/utctf/suspicious$ ls
breifcase.jpg
user@kali:~/Downloads/utctf/suspicious$ file breifcase.jpg
breifcase.jpg: JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 750x750, compo
nents 3
```

It’s a briefcase, so let’s see if there’s something inside?



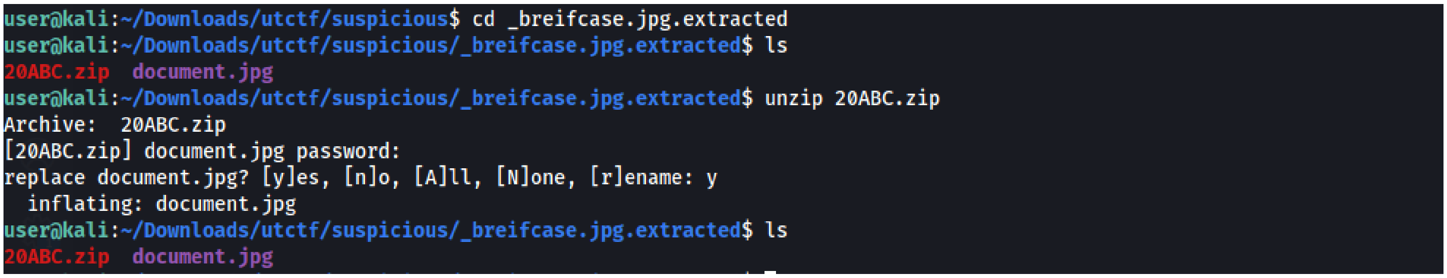
```
user@kali:~/Downloads/utctf/suspicious$ binwalk breifcase.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
2236          0x8BC           Copyright string: "CopyrightOwner> <rdf:Seq/> </plus:CopyrightOwner> <plus:Licensor> <rdf:Seq/> </plus:Licensor>
</rdf:Description> </rdf:RDF> </x:"
2270          0x8DE           Copyright string: "CopyrightOwner> <plus:Licensor> <rdf:Seq/> </plus:Licensor> </rdf:Description> </rdf:RDF> </x:
xmpmeta>  "
133820        0x20ABC         Zip archive data, encrypted at least v2.0 to extract, compressed size: 31357, uncompressed size: 44434, name: doc
ument.jpg
165345        0x285E1         End of Zip archive, footer length: 22
```

I extract the embedded files into another directory.



```
user@kali:~/Downloads/utctf/suspicious$ binwalk -e breifcase.jpg
```

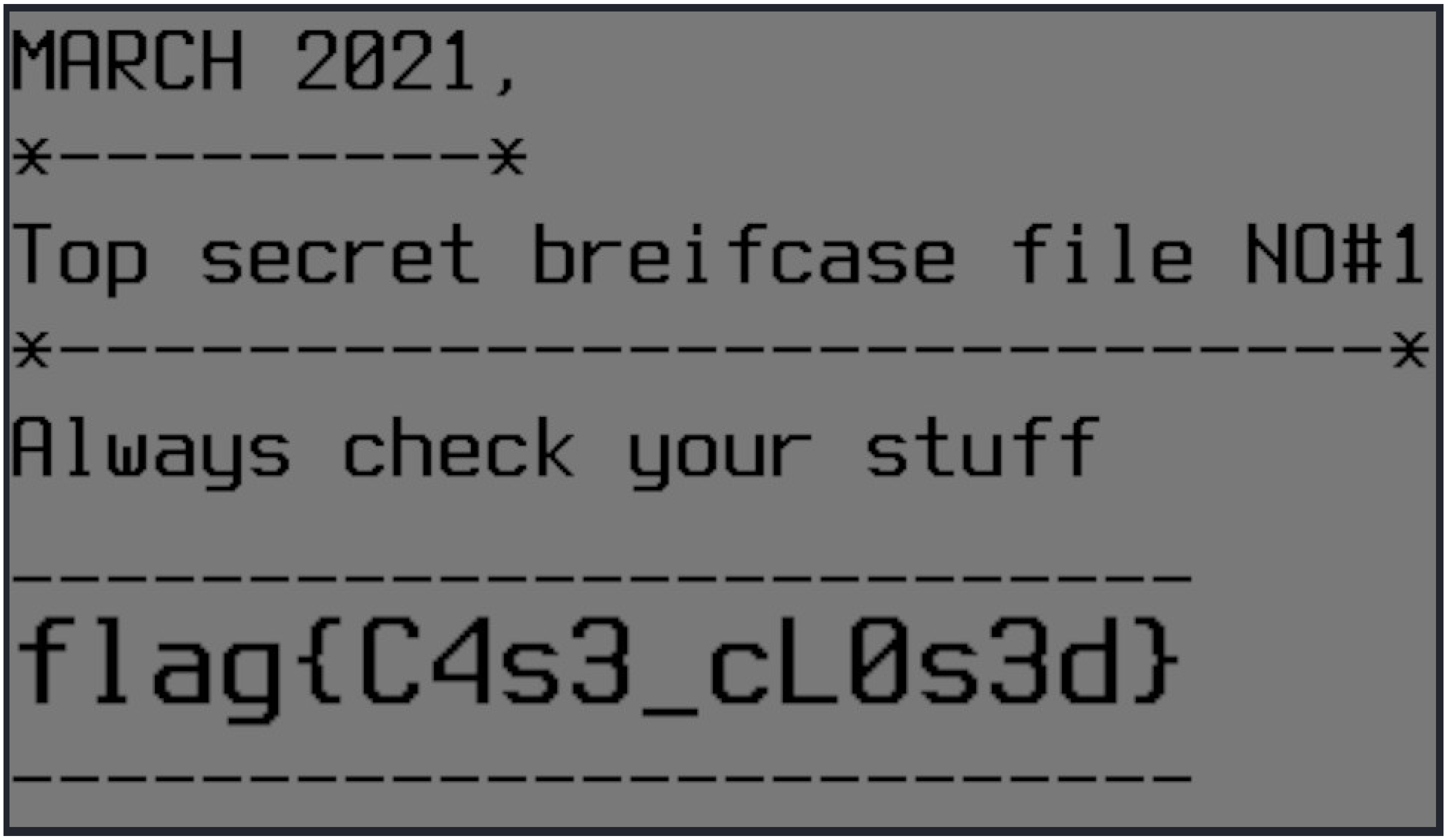
This gives us an encrypted image and a zip archive, but it’s password protected! Let’s try the string on the briefcase?



```
user@kali:~/Downloads/utctf/suspicious$ cd _breifcase.jpg.extracted
user@kali:~/Downloads/utctf/suspicious/_breifcase.jpg.extracted$ ls
20ABC.zip  document.jpg
user@kali:~/Downloads/utctf/suspicious/_breifcase.jpg.extracted$ unzip 20ABC.zip
Archive:  20ABC.zip
[20ABC.zip] document.jpg password:
replace document.jpg? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: document.jpg
user@kali:~/Downloads/utctf/suspicious/_breifcase.jpg.extracted$ ls
20ABC.zip  document.jpg
```

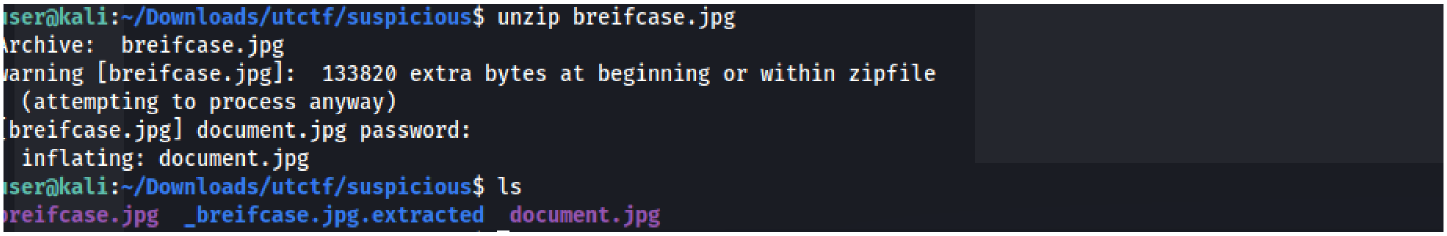
That looks interesting!

Navigating to the file presents us with the flag!



```
MARCH 2021,
*---------*
Top secret breifcase file NO#1
*----------------------------*
Always check your stuff

_________________________
flag{C4s3_cL0s3d}
_________________________
```

We could also just unzip the briefcase without the extra steps. Easy!



```
ser@kali:~/Downloads/utctf/suspicious$ unzip breifcase.jpg
rchive:  breifcase.jpg
arning [breifcase.jpg]:  133820 extra bytes at beginning or within zipfile
  (attempting to process anyway)
breifcase.jpg] document.jpg password:
  inflating: document.jpg
ser@kali:~/Downloads/utctf/suspicious$ ls
reifcase.jpg  _breifcase.jpg.extracted  document.jpg
```