

Something Shady, Maybe

50

To test out his skills, Amn Snuffy's supervisor gave him a file for analysis. He needs to determine if the file is malicious. As a strter, Amn Snuffy notices that the file size is somewhat big for a simple image. Do you think there is more to it? Can you help him out? First, how many files are there?

Unlock Hint for 10 points

123.zip

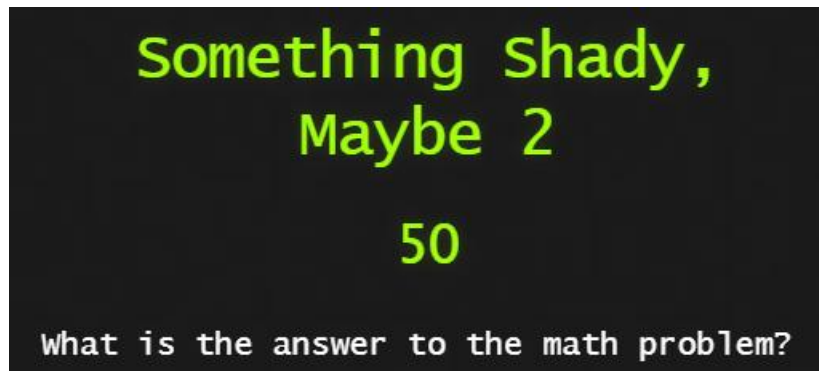
We get a zip file with a single image inside of it.

I moved this over to a kali box and ran the unzip command on the file to look for other files hidden inside the jpg.

```
kali@kali:~/5charlie/123$ unzip dontlook.jpg
Archive:  dontlook.jpg
warning [dontlook.jpg]: 18328 extra bytes at beginning or within zipfile
(attempting to process anyway)
  inflating: 1
  inflating: .2
  inflating: .3
  inflating: .4
  inflating: .5
kali@kali:~/5charlie/123$ mv .2 2
kali@kali:~/5charlie/123$ mv .3 3
kali@kali:~/5charlie/123$ mv .4 4
kali@kali:~/5charlie/123$ mv .5 5
kali@kali:~/5charlie/123$ file *
1:      PDF document, version 1.6
2:      ASCII text, with no line terminators
3:      PNG image data, 857 x 703, 8-bit/color RGBA, non-interlaced
4:      ASCII text
5.doc:  Microsoft Word 2007+
dontlook.jpg: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1,
```

Plus the two dontlookhere.jpg files you get a total of 7 files

Flag: 7



We look at the files and see that there are some hidden items and one of those is an encrypted pdf and a couple of text files.

.2 is some base 64 encoding

RW1pbmVtSXNNYXJzaGFsbEJydWNITWF0aGVyc0lJSWFuZFNsaW1TaGFkeQ==

The screenshot shows a web-based Base64 decoder. On the left, the 'Recipe' panel is set to 'From Base64' with the alphabet 'A-Za-z0-9+/' and the option 'Remove non-alphabet chars' checked. The 'Input' field contains the Base64 string 'RW1pbmVtSXNNYXJzaGFsbEJydWNITWF0aGVyc0lJSWFuZFNsaW1TaGFkeQ=='. The 'Output' field displays the decoded result: 'EminemIsMarshallBruceMathersIIIandSlimShady'.

Which translates to: EminemIsMarshallBruceMathersIIIandSlimShady

But the password is actually the b64 text

Amn Bagodonuts chose a number, multiplied it by 2, then subtracted 138 from the result and got 102.
What was the number he chose?



$X * 2 - 138 = 102$ what is x?

X=120

Flag: 120

Something Shady,
Maybe 3

80

Which Doctor is missing?

Unlock Hint for 16 points

Looking at the file we see on the last page a b64 encoded flag:

```
Flag{YUhSMGNITTZMeTkzZDNjdWVXOTFkSFZpWIM1amlyMHZkMkYwWTJnL2RqMWxTazgxU0ZWZk4xO  
Hhkdz09}
```

Decode that:

```
aHR0cHM6Ly93d3cueW91dHVizS5jb20vd2F0Y2g/dj1lSk81SFVfN18xdw==
```

Decode the b64 again

Output

```
https://www.youtube.com/watch?v=eJ05HU_7_1w
```

Follow the link: (hoping its not a rick roll!!!)



Flag: Dr. Dre