First, what I did is open the file with 7zip, to see if there is anything inside. It seems there is a decompiled apk somewhere, so I decide to delve deeper with volatility.

After finding a suitable profile with image info, I looked for any existing apks:

```
┌──(kali㉿kali)-[/tmp/VMwareDnD/n7L1ht]
└─$ vol.py -f spyagency3.bin --profile=Win7SP1x64 filescan | grep ".apk"
Volatility Foundation Volatility Framework 2.6.1
0x000000003debe530     16      0 RW---- \Device\HarddiskVolume2\Users\volf\Documents\app-release.apk.zip
0x000000003fa82210     16      0 RW---- \Device\HarddiskVolume2\Users\volf\Downloads\app-release.apk.zip
0x000000003fc503c0     16      0 RW---- \Device\HarddiskVolume2\Users\volf\Desktop\app-release.apk - Copy.zip
0x000000003fefb8c0     16      0 R--r-- \Device\HarddiskVolume2\Users\volf\Desktop\app-release.apk.zip
```

```
┌──(kali㉿kali)-[/tmp/VMwareDnD/n7L1ht]
└─$ vol.py -f spyagency3.bin --profile=Win7SP1x64 dumpfiles -D /home/kali/Desktop/ -Q 0x000000003debe530
vol.py -f spyagency3.bin --profile=Win7SP1x64 dumpfiles -D /home/kali/Desktop/ -Q 0x000000003fa82210
vol.py -f spyagency3.bin --profile=Win7SP1x64 dumpfiles -D /home/kali/Desktop/ -Q 0x000000003fc503c0
vol.py -f spyagency3.bin --profile=Win7SP1x64 dumpfiles -D /home/kali/Desktop/ -Q 0x000000003fefb8c0

Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3debe530   None   \Device\HarddiskVolume2\Users\volf\Documents\app-release.apk.zip
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fa82210   None   \Device\HarddiskVolume2\Users\volf\Downloads\app-release.apk.zip
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fc503c0   None   \Device\HarddiskVolume2\Users\volf\Desktop\app-release.apk - Copy.zip
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fefb8c0   None   \Device\HarddiskVolume2\Users\volf\Desktop\app-release.apk.zip
```

Only the 4th command actually extracts the decompiled apk, for some reason. In any case, the next part of the challenge involves exploring the decompiled application.

The logic seems to be basic, so we look through the res folder and… we find a file named **coordinates_can_be_found_here.jpg**. It is an image of a gps, however that's a red herring. The coordinates we need can be found in the exifdata, under a comment. It points to a pizza hut location in Bucharest. After various attempts, the answer is **ctf{sha256{pizzahut)}**

Made with love by: AndreiCat