

## Initiale Analyse

Gegeben ist ein Bild `doggo.jpg`, welches einen Hund zeigt.



Figure 1: `doggo.jpg`

Wir sind allerdings auf der Suche nach einer Flagge, also müssen wir weiter suchen!

Die Aufgabe ist in der Kategorie Steganographie, wobei Steganographie die Kunst bezeichnet, Informationen in einem anderen Medium versteckt einzubetten. Irgendwo in der Datei muss also die Flagge versteckt sein.

## Analyse der Metadaten

Das Bild enthält zum Beispiel in Form von Metadaten noch einige augenscheinlich versteckte Informationen. Unter Linux können wir uns diese mit dem Tool `exiftool` anzeigen lassen:

```
$ exiftool doggo.jpg
ExifTool Version Number      : 12.70
File Name                    : doggo.jpg
[...]
Device Manufacturer         : Apple Computer Inc.
Device Model                 :
Device Attributes           : Reflective, Glossy, Positive, Color
Rendering Intent             : Perceptual
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator              : Apple Computer Inc.
[...]
Image Width                  : 2078
Image Height                 : 3128
[...]
```

Hmm, wir wissen zwar, dass das Bild anscheinend mit einem Apple Gerät aufgenommen wurde und 3128 Pixel hoch ist, allerdings sind wir der Flagge noch keinen Schritt näher gekommen.

## Lösung

Wir suchen in dem Bild nach einer Zeichenkette, welche die Form `SSH{...}` hat. Unter Linux können wir mit dem Tool `strings` uns alle Zeichenketten ausgeben lassen, die in einer Datei enthalten sind. Wenn wir dem Tool unser Bild geben, erhalten wir viele kryptisch aussehende Zeichenketten. Das liegt daran, dass das

Bild zufällig Werte enthalten kann, die in dem Wertebereich von normalen Zeichen liegen und deswegen von dem Tool mit ausgegeben werden.

```
$ strings doggo.jpg
[...]  
`~wN  
SSH{th3r3s_m0r3_th4n_4_cut3_p1c7ur3}
```

Da ist die Flagge! Die Flagge steckte schon als Zeichenkette im Bild. Wenn wir die Datei mit einem Hexeditor oder einem gewöhnlichen Texteditor öffnen, würden wir auch sehen können, dass die Flagge die letzten Bytes der Datei sind.

## Interessante Links

Folgende Webseite enthält eine Zusammenfassung für einige Steganographie Tricks, die bei CTF Aufgaben helfen können: <https://book.hacktricks.xyz/crypto-and-stego/stego-tricks>