

Information

This CTF challenge that I worked on involved cat.jpg, where the hint was "look at the details of the file." After closer inspection, the image looked legitimate, but after analyzing its information through exiftool and looking through its raw data through xxd, it indeed contained a Base64 string: "cGljb0NURnt0aGVfbTN0YWRhdGFfMXNfbW9kaWZIZWR9." Which, after decoding, returned "picoCTF{the_m3tadata_1s_modified}." The lesson to take away from this challenge is how flags can hide themselves away from the raw information contained within a document, and how it is relatively straightforward after employing the aid of commands such as 'file', 'exiftool'.