## Did you notice...?

Forensics

This is a write-up for the forensics challenge from 09.12.2023 [Did you notice...?](https://cyberxmas.milestone.dk/challenges#Did%20you%20notice...?-45):

*This flag is lying around for a while, don't pretend you don't know about it.*

*Note: enter the flag in reverse order MilestoneCTF{abc1234} -> MilestoneCTF{4321cba}*

From the challenge description it was obvious that we were already given the flag and we had missed it previously. Only logical thing that we had supplied before the challenges started was the “Get ready for the CyberXmas 2023!” email.

That mail contained a text poem and a image – we had already used the poem and found the flag there for another challenge – Cyber Xmas Carols. That left only the image attached – **ctf23.jpg**

****

I like image challenges so I immediately started:

First thought was steganography! I have a very good tool for solving those quick and easy - <https://github.com/Giotino/stegsolve>, fired it up, loaded the jpg file inside and started switching options there – it does almost all things needed for steganography challenge:

* Colour inversion (xor)
* Extracting and showing separate colour/alpha planes
* Random colour maps
* Full gray/color
* Pixel offset
* File (exif) information
* Etc.

Nevertheless these showed nothing, worthless images for our task:

A screenshot of a computer

Description automatically generated

I moved on, I decided to check if the [exiftool](https://github.com/exiftool/exiftool) will show something that stegsolve missed:

A screenshot of a computer program

Description automatically generated

Its not here, okay!

Lastly I checked through my tools and found [steghide](https://github.com/StefanoDeVuono/steghide) – a quick jump on the CyberXmas Tools page showed that same one as well – okay we can be onto something!

First run of the tool – not much, it requires an passphrase, hmmm:



What could it be… But I did not search it for a very long time, there was something in the CyberXmas mail that was obvious hint since I received the mail:

A green background with white text

Description automatically generated

OK! I run the steghide, this time providing “hohoho!” as pass:

A black and blue text

Description automatically generated

A winner! I quickly open the flag.txt file and we have the flag!

**MilestoneCTF{hiding-in-a-plain-sight-as-usual}**

One last step before we enter it though! We have to reverse the flag as per the requirements of the challenge! I go to [CyberChef](https://gchq.github.io/CyberChef/) and use the reverse operation:

}lausu-sa-thgis-nialp-a-ni-gnidih{FTCenotseliM

And the answer is accepted!

The end.