***CRYPTONITE***

**FORENSICS**

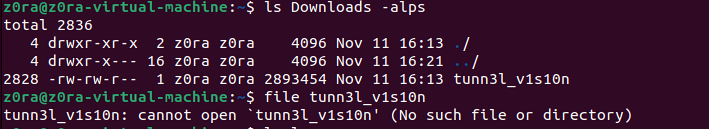
Name – Kunal Komre

Registration Number- 230932186

I started the forensics by, of course, learning about it. Digital Forensics is the process of identifying, preserving, analysing and presenting digital evidences.

**1ST TASK**

***tunn3l v1s10n***



The file does not open when I try to open it terminal

So I opened the file with an online hex editor.

The hex editor showed that it starts with BM, so this might be a BMP file.

BMP is an image file format that contains bitmap graphics data

I tried to open the image but it didn’t work this means the file is corrupted.

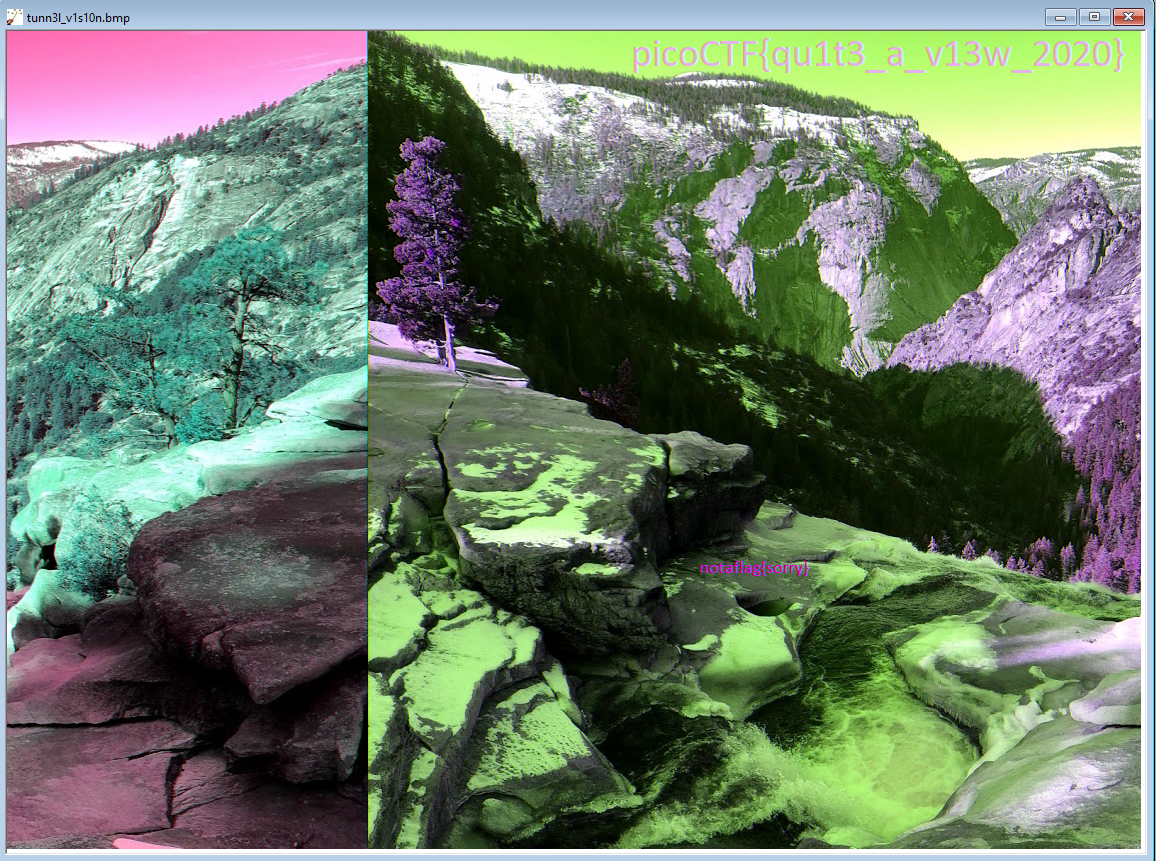
I compared the BMP file with another BMP file to see if there are any similarities.

It showed that some values were different from normal which prevented the file from opening.

I changed the values of BA D0 – BA D0 to 36 00 – 28 00



Image showed a flag but not in the format of picoctf



Final ctf – picoctf{qu1t3\_a\_v13w\_2020}

**Trivial FTP**

A pcapng file was downloaded

PCAPNG (PCAP Next Generation) is more extensible and portable than PCAP and has a more flexible file structure. It also includes additional information about the packet, and the interface used to capture the packet, such as drop counters, DNS records, etc.

The pCAPng file was not opeining

I had to download Wireshark to complete the task.

After opening the file I was shown the bmp images. They were just scenic views.

I opened intructions.txt and copied the text and went to ROT13 to decipher them.



It told me to check the plan file. I had to decipher it again.

It told to use program.deb along with the password being DUEDILIGENCE.

I don’t completely understand why but we had to use the steghide command to decipher the images and get the flag.

I used steghide command on all images but only picture3 responded

Command used :- steghide extract -sf pictures.bmp -p DUEDILIGENCE

Picture3 contained the flag and I got it using cat flag.txt

**FINAL FLAG:-** picoCTF{h1dd3n\_1n\_pLa1n\_51GHT\_18375919}

**MACROHARD WEAKEDGE**

I downloaded the pptm file. It showed the message ‘Forensics is fun’

I extracted the files and got a code which seemed in base64

I decoded the code and got the flag

**FINAL FLAG:-** picoCTF{D1d\_u\_kn01\_ppts\_r\_z1p5}