**Forensics**

**1.Welcome**

In this challenge we are given an image which contains a zip file. When we extract this zip file, we can find zip in a zip file for two times, then we can find a file named “secret.bmp”. When we do strings on that file (actually it’s not a bitmap) , we can find a base64 string as “dGhlIHBhc3N3b3JkIGlzOiBoMzExMF90aDNyMyE==”. By decrypting this base64 string, we can get the password as “h3110\_th3r3!”. This is the password for the zip file called “a.zip”.

After opening the zip file, we will get a PNG called “a.png”.

By using stegsolve on “a.png”, we can get the flag in Red plane1.

The flag is: “pctf{st3gs0lv3\_1s\_u53ful}”

**2.Magic PNGs**

In this challenge we are given a password protected zip file and a corrupted PNG image. The PNG image can be corrected by changing the critical chunk from “idat” to “IDAT” and correcting the header file signature into “89 50 4E 47 0D 0A 1A 0A”. Then the PNG file is uncorrupted. The PNG image has the text as “h4CK3RM4n” in inverted and flipped format. According to the hint , we can find the md5 hash of above secret word as “**2c919f82ee2ed6985d5c5e275d67e4f8**”. This is the password for the given zip file from which we can get the flag.

The flag is: “pctf{y0u\_s33\_m33\_n0w!}”

**3.Save Earth**

In this challenge a USB keyboard capture. In the capture , I considered “2” as “-” , “4” as “.” and “1” as “space” , we can get a morse as “-.-. - ..-. ... ....- ...- ...--” , which can be translated as “CTFS4V3”.

The flag is: “ctfs4v3”

**4.Slow Realization**

In this challenge, we are given a zip file which contains a pdf and a jpeg image. An mp3 file is embedded in the jpeg image. The header for mp3 file is “ID3”. We can carve the mp3 file by seeing the offset of “ID3”. Then the obtained mp3 file can be seen under spectrographic view which contained the morse code. After decoding the morse, we get “patienceisthekeypctfn0th3r3”.

In the middle of morsecode , we can find an audio sample whose properties can be adjusted so that we can hear that. Then the we can get the password as “congratulations”.

However, if we use rockyou.txt on the pdf file using pdfcrack , we can get the password as “congratulations”.

The flag can be found in the pdf file.

The flag is : “pctf{y0u\_h34rd\_m3\_r1ght}”