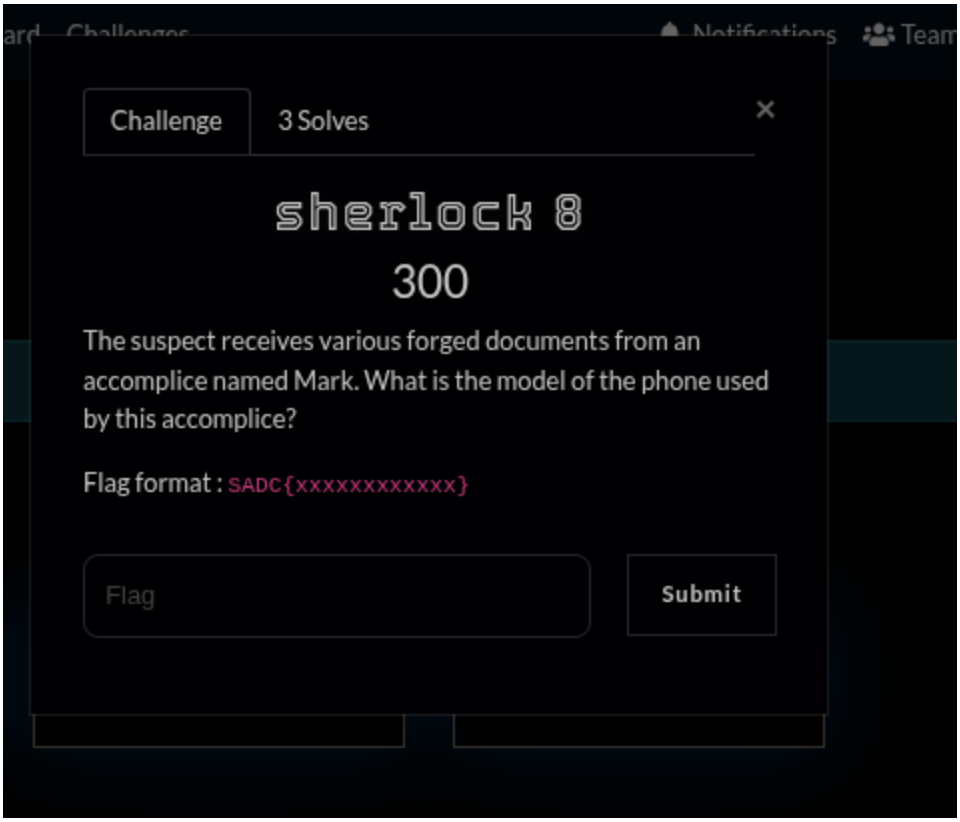


- This was an interesting challenge and was happy to draw `first blood` on the challenge and this had many days without anyone figuring it out
- The challenge was based on `Android` phone `data` that was presented after downloading a `.rar` folder
- After downloading the `data.rar` folder in my `kali` box i unzipped

```
┌──(mayday㉿kali)-[/dev/shm]
└─$ unrar x data.rar
```

- The folder was successfully un-archived, i then navigated to the folder to investigate it further. The sheer amount of the folder was confusing

```
┌──(mayday㉿kali)-[/dev/shm/data]
└─$ ls
adb       app-ephemeral  bootchart     fonts               lost+found  misc_de   property                ss          unencrypted  vendor_de
anr       app-lib        cache         gsi                 media       nfc       resource-cache          system      user
apex      app-private    dalvik-cache  gsi_persistent_data  mediadrm    ota       rollback-history        system_ce   user_de
app       app-staging    data          incremental         misc        per_boot  rollback-observer       system_de   vendor
app-asec  backup         drm           local               misc_ce     preloads  server_configurable_flags  tombstones  vendor_ce
```

- The first idea that came to my mind was let me `grep` the flag out of these folders :)
- I stumbled upon this and thought this was the flag

```
data/com.google.android.gms/shared_prefs/nearbysharing_service_state.xml
3:Galaxy S3
```

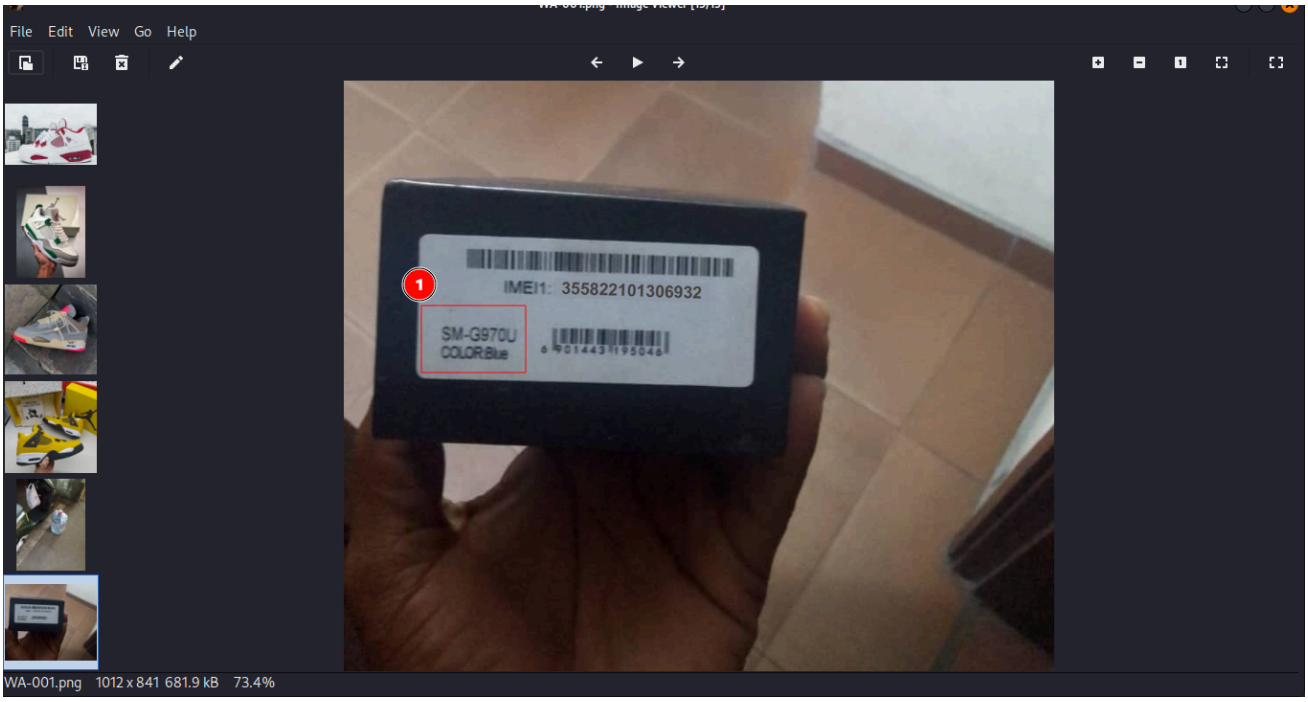
- After several attempts to grep the data out of the folders , i realized i was not going anyway, and also after seeing that some of the folders inside had nothing in them a thought struct me, *what if i can arrange the folders according to size?*
- I went back to my terminal and arranged the folders to check them by size

```
└─$ du -h --max-depth=1 2>/dev/null | sort -hr | head -20
2.0G    .
1.1G    ./app
328M    ./media
308M    ./data
147M    ./user
95M     ./user_de
11M     ./system
7.4M    ./dalvik-cache
6.8M    ./misc
3.5M    ./anr
664K    ./system_ce
204K    ./misc_de
184K    ./system_de
140K    ./misc_ce
132K    ./backup
72K     ./vendor
52K     ./resource-cache
44K     ./unencrypted
4.0K    ./property
0       ./vendor_de
```

- From the sizes i started from the highest in size
- After several efforts going inside the folder i stumbled on this folder `/media/0/WhatsApp/Media/WhatsApp Images`
- In the folder there were numerous images

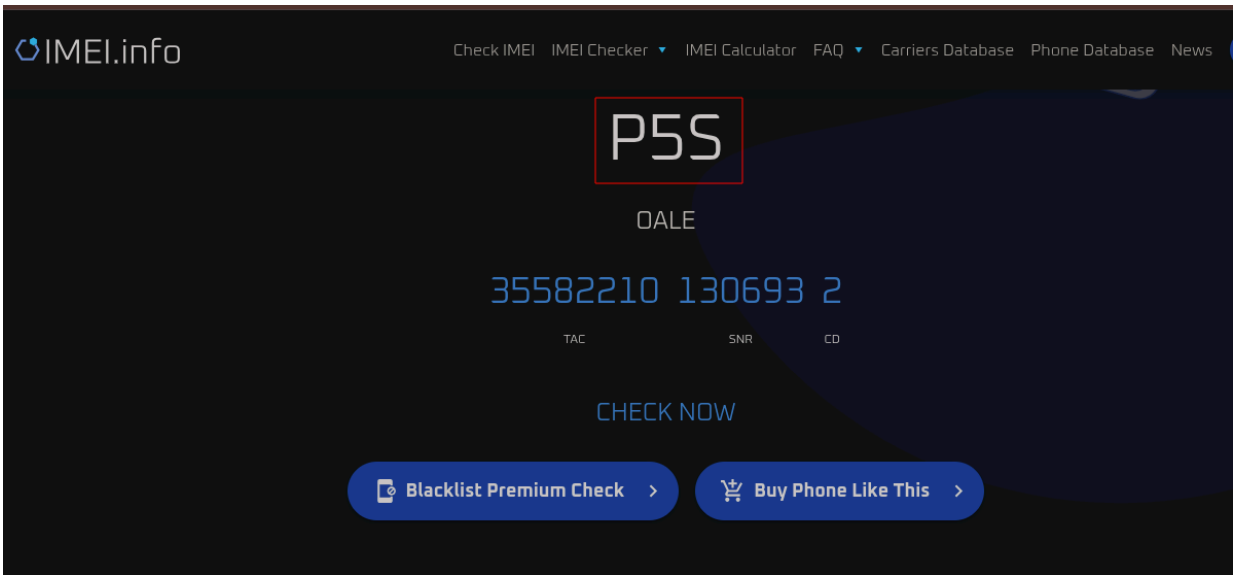
```
┌──(mayday㉿kali)-[/dev/…/0/WhatsApp/Media/WhatsApp Images]
└─$ ls
IMG-20231020-WA0000.jpg  IMG-20231020-WA0003.jpg  IMG-20231020-WA0006.jpg  IMG-20231020-WA0019.jpg  IMG-20231021-WA0026.jpg  IMG-20231021-WA0029.jpg  Private
IMG-20231020-WA0001.jpg  IMG-20231020-WA0004.jpg  IMG-20231020-WA0007.jpg  IMG-20231021-WA0000.jpg  IMG-20231021-WA0027.jpg  IMG-20231021-WA0030.jpg  Sent
IMG-20231020-WA0002.jpg  IMG-20231020-WA0005.jpg  IMG-20231020-WA0008.jpg  IMG-20231021-WA0021.jpg  IMG-20231021-WA0028.jpg  IMG-20231027-WA0001.jpg  WA-001.png
```

- I opened my image viewer here and started checking the images, some of the images did not make sense , and *yes* i did run `exiftool` on them to check their metadata but to no avail
- I found this image rather intruiging



- The first attempt was think probably the `model` is samsung since i had previously seen the `galaxy` tag
- i google the model and still this was a dead end, i did not know that i was staring at the `answer`, Did you see it ? i bet not well here

- I went to google to search for an `IMEI` service to view the model
- I stumbled upon this website
- I entered the `IMEI` code and found this



- Here i got the model and this was the flag `SADC{PS5}`
- I hope you enjoyed