* Unzip berkas **Kasus.zip** menggunakan password yang telah diberikan oleh panitia.
* Setelah di unzip ada dua berkas yaitu **soal.txt** dan **system.img**
* Dari soal diketahui bahwa kami diharuskan untuk menganalisa dan mendapatkan flag dalam berkas **system.img**
* Dari pengecekan dengan menggunakan perintah **file**, diketahui bahwa **system.img** merupakan sebuah berkas file system berformat **Fat16**

**file system.img**

system.img: x86 boot sector, code offset 0x3c, OEM-ID "MSWIN4.1", sectors/cluster 8, reserved sectors 304, root entries 512, Media descriptor 0xf8, sectors/FAT 192, heads 1, sectors 389632 (volumes > 32 MB) , serial number 0x4d23f3f1, unlabeled, FAT (16 bit)

Selanjutnya adalah melakukan mount file **system.**img ke sebuah direktori dilakukan dengan perintah-perintah ini:

**mkdir temp**

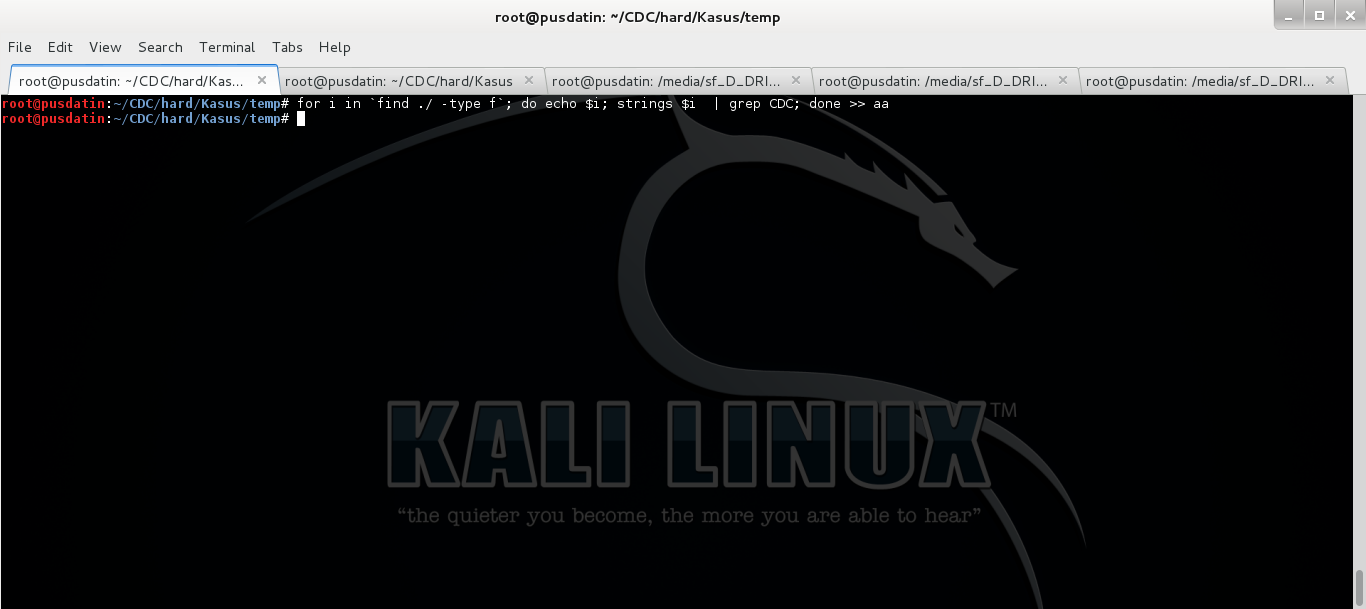
**mount –o loop system.img ./temp**

**cd ./temp**

**ls –lha ./temp**

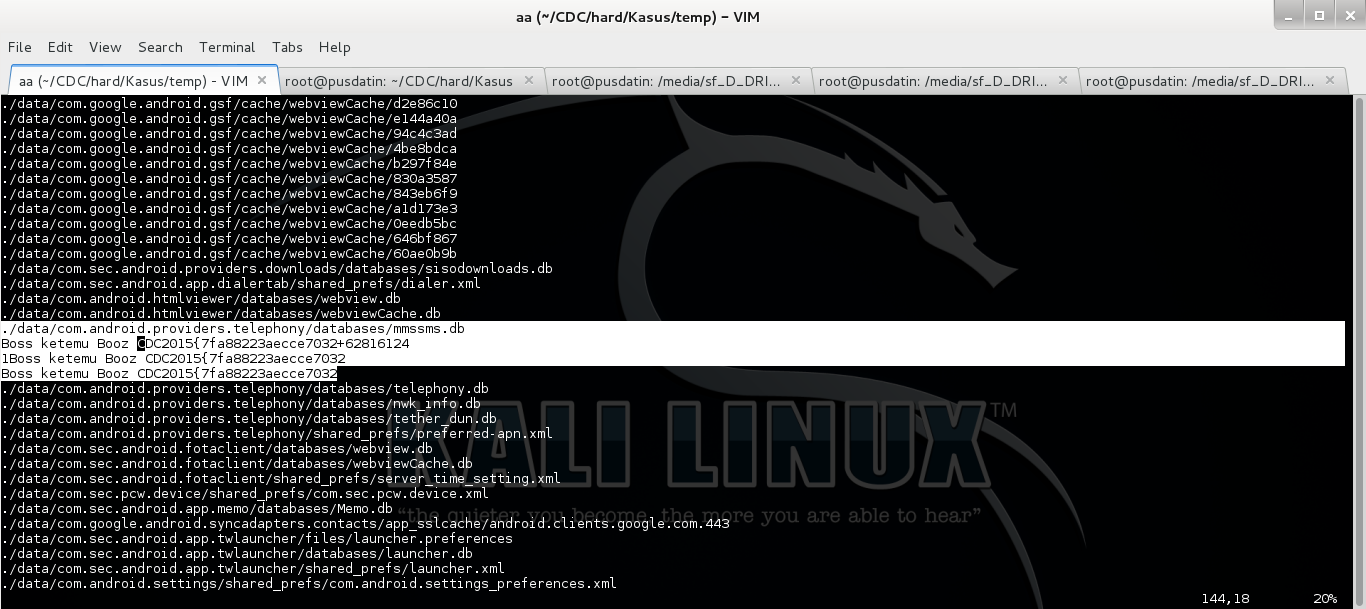
* Berkas **system.img** sekarang sudah termounting di direktori ./temp.
* Selanjutnya adalah melakukan analisa semua berkas yang ada di direktori ./temp.

Analisa yang dilakukan adalah mencari keyword CDC dan dibuang ke sebuah file bernama **aa**



**for i in `find ./ -type f`; do echo $i; strings $i | grep CDC; done >> aa**

Selanjutnya adalah menganalisa berkas aa



dan didapatkan berkas

**./data/com.android.providers.telephony/databases/mmssms.db**

**./data/com.sec.android.provider.logsprovider/databases/logs.db**

**./data/com.whatsapp/lib/libwhatsapp.so**

**./data/com.whatsapp/databases/msgstore.db**

Yang dicurigai mengandung flag.

Berkas tersebut berformat sqllite sehingga bisa dilihat isinya. Setelah dicek menggunakan sqlite browser (<http://sqlitebrowser.org/>) diduga flag ada pada berkas

**./data/com.whatsapp/databases/msgstore.db**

Dari pengecekan kemungkinan Flag berupa gambar di URL sebagai berikut:

<https://mmi646.whatsapp.net/d/4COD2pW9T9yjkGb4SiPCcVUHZfIABRFwI1KWJQ/AkunWptvhbetHCgJTIYCmM2pjrP4_OHdu2XMbbtanb8c.jpg>

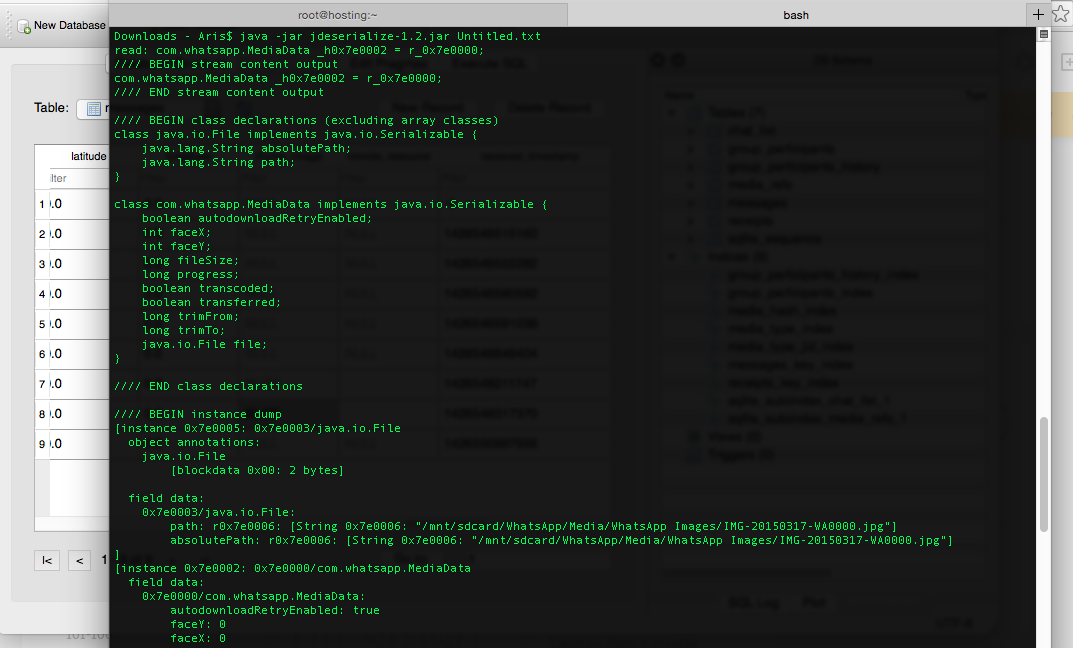
<https://mmi646.whatsapp.net/d/fbKMLkkuf1zdavcAued9H1UHZl0ABRFwKbURRQ/AkunWptvhbetHCgJTIYCmM2pjrP4_OHdu2XMbbtanb8c.jpg>

Dalam database sqllite jg ada tipe data dalam format BLOB, kemungkinan besar gambar tersebut bisa dibuka.

Dari hasil pengecekan ternyata file blob tersebut adalah JD Serialize dan bisa dibuka dengan menggunakan JDSerialize (<https://code.google.com/p/jdeserialize/wiki/Documentation>)

Yang pertama dilakukan ada mengeksport file blob tersebut menjadi Untitled.txt

**java –jar jdserialize-1.2.jar Untitled.txt**



Kemungkinan besar flag terletak pada direktori

**/mnt/sdcard/WhatsApp/Media/WhatsApp Images/IMG-20150317-WA0000.jpg**