[Capture The Flag]

NAMA TIM : [KOTAK-HITAM - SMKN 1 BATAM]

Rabu 21 October 2020

Ketua Tim	
1.	Jean Tirstan
Member	
1.	Joy Gilbert
2.	

FORENSIC

File Signature (LKS-SMK 28)

Diberikan sebuah sebuah file yang mencurigakan, diperkirakan file ini extention nya diganti dan ada data yang hilang di file signature nya. Diketahui bahwasanya extensinya berbeda setelah kita cek menggunakan file

```
0ncom@kali:~/Downloads/CTF_LKS2020$ file flag.jpg.exe.doc.rar
flag.jpg.exe.doc.rar: RAR archive data, v5
0ncom@kali:~/Downloads/CTF_LKS2020$
```

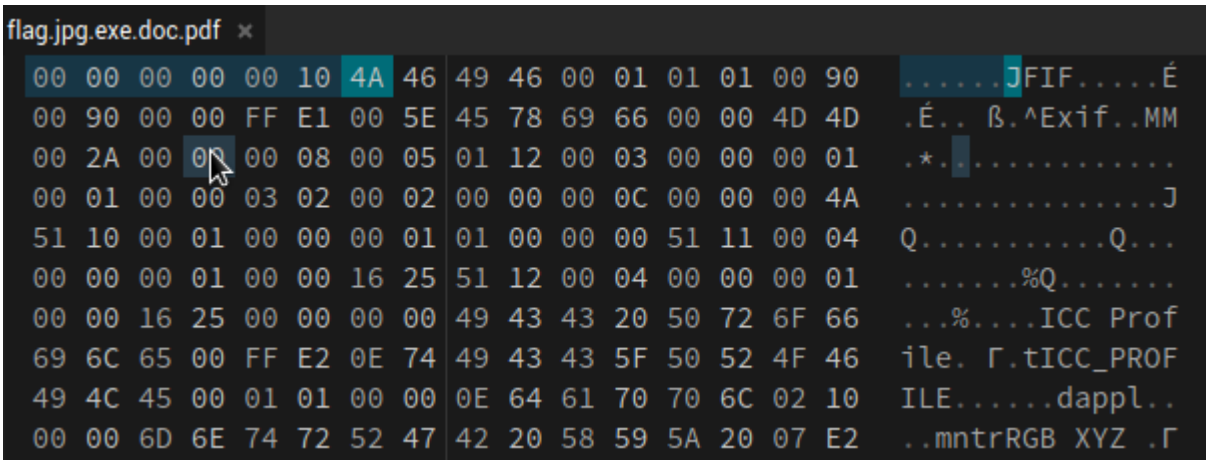
Diketahui dari string yang telah kami test extensinya addalah JPG

```
0ncom@kali:~/Downloads/CTF_LKS2020$ file flag.rar
flag.rar: RAR archive data, v5
0ncom@kali:~/Downloads/CTF_LKS2020$ file flag.jpg.exe.doc.pdf
flag.jpg.exe.doc.pdf: data
0ncom@kali:~/Downloads/CTF_LKS2020$ strings ./flag.jpg.exe.doc.pdf | head -10
JFIF
^Exif
ICC Profile
tICC_PROFILE
dappl
mntrRGB XYZ
acspAPPL
APPL
-appl
desc
0ncom@kali:~/Downloads/CTF_LKS2020$
```

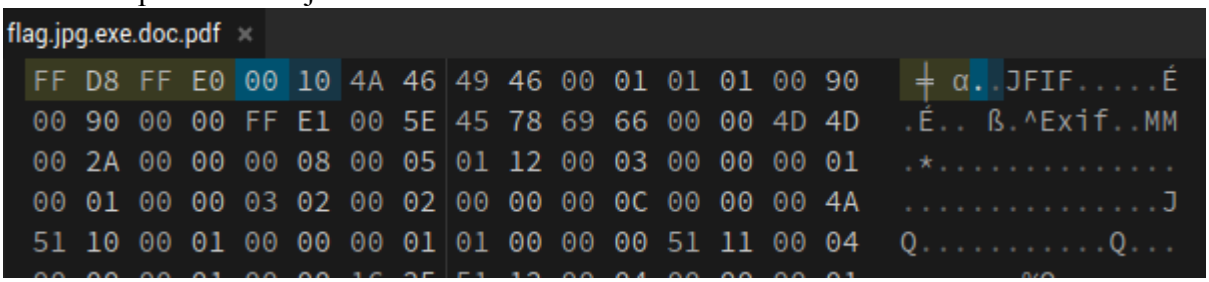
Dan disini adalah awalan extensinya memiliki kesalahan

```
0ncom@kali:~/Downloads/CTF_LKS2020$ hexdump ./flag.jpg.exe.doc.pdf | head -10
0000000 0000 0000 1000 464a 4649 0100 0101 9000
0000010 9000 0000 e1ff 5e00 7845 6669 0000 4d4d
0000020 2a00 0000 0800 0500 1201 0300 0000 0100
0000030 0100 0000 0203 0200 0000 0c00 0000 4a00
0000040 1051 0100 0000 0100 0001 0000 1151 0400
0000050 0000 0100 0000 2516 1251 0400 0000 0100
0000060 0000 2516 0000 0000 4349 2043 7250 666f
0000070 6c69 0065 e2ff 740e 4349 5f43 5250 464f
0000080 4c49 0045 0101 0000 640e 7061 6c70 1002
0000090 0000 6e6d 7274 4752 2042 5958 205a e207
0ncom@kali:~/Downloads/CTF_LKS2020$
```

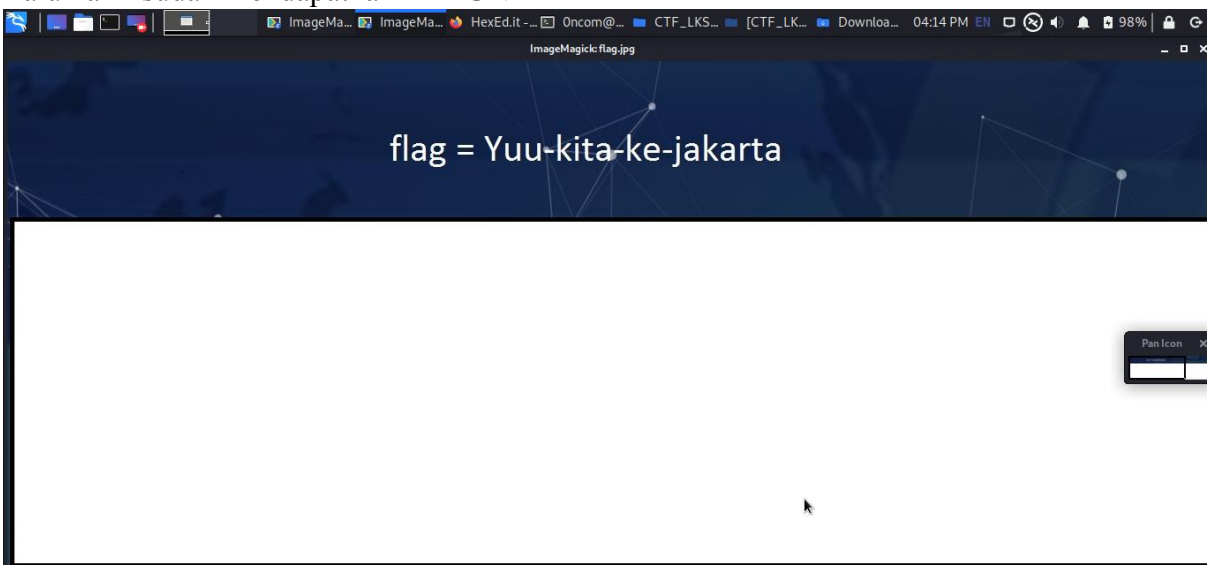
Dibawah ini adalah extensi file signature yang masih salah.



Setalah di perbaiki menjadi FF D8 FF E0 00 10 4A 46 49 46 00 01



Lalu kami sudah mendapatkan FLAGNYA



FLAG = {Yuu-kita-ke-jakarta}

gambar1

Diberikan sebuah gambar seperti dibawah untuk menemukan hash MD5 gambar tersebut.

```
0ncom@kali:~/Downloads/CTF_LKS2020$ md5sum 2018-09-22_09.31.07.jpg
c0b7d53ada2ad6858df4ada15f40b550  2018-09-22_09.31.07.jpg
0ncom@kali:~/Downloads/CTF_LKS2020$
```

Kami langsung saja mengeksekusinya menggunakan md5sum

FLAG = LKSSMK28{ c0b7d53ada2ad6858df4ada15f40b550}

Gambar2

Untuk soal gambar2 kita tetap menggunakan gambar yang diberikan pada soal gambar1,tetapi untuk soal gambar2 ini kita disuruh untuk mengerjakan mencari tanggal foto tersebut.

```
0ncom@kali:~/Downloads/CTF_LKS2020$ exiftool 2018-09-22_09.31.07.jpg
ExifTool Version Number         : 12.07
File Name                       : 2018-09-22_09.31.07.jpg
Directory                       : .
File Size                       : 1319 kB
File Modification Date/Time     : 2020:10:21 17:04:57+07:00
File Access Date/Time           : 2020:10:21 17:04:57+07:00
File Inode Change Date/Time     : 2020:10:21 17:04:57+07:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
Exif Byte Order                 : Big-endian (Motorola, MM)
Resolution Unit                 : inches
Make                            : LGE
Camera Model Name               : Nexus 5X
Software                        : bullhead-user 8.1.0 OPM6.171019.030.K1 4947289
 release-keys
Modify Date                     : 2018:09:22 09:31:08
Orientation                     : Horizontal (normal)
Y Cb Cr Positioning             : Centered
ISO                             : 50
Exposure Program                : Not Defined
F Number                        : 2.0
Exposure Time                   : 1/237
Sensing Method                  : Unknown (0)
Sub Sec Time Digitized          : 403858
Sub Sec Time Original           : 403858
Sub Sec Time                    : 403858
Subject Distance Range          : Distant
Focal Length                    : 2.6 mm
Flash                           : No Flash
Metering Mode                   : Unknown
Scene Capture Type              : Standard
Interoperability Index          : R98 - DCF basic file (sRGB)
Interoperability Version        : 0100
Focal Length In 35mm Format     : 0 mm
Create Date                     : 2018:09:22 09:31:08
Exposure Compensation           : 0
```

Pada gambar diatas tersebut kami menggunakan langsung perintah exiftool,lalu akan menemukan kapan foto itu dilakukan (tanggal,bulan,tahun serta waktunya)

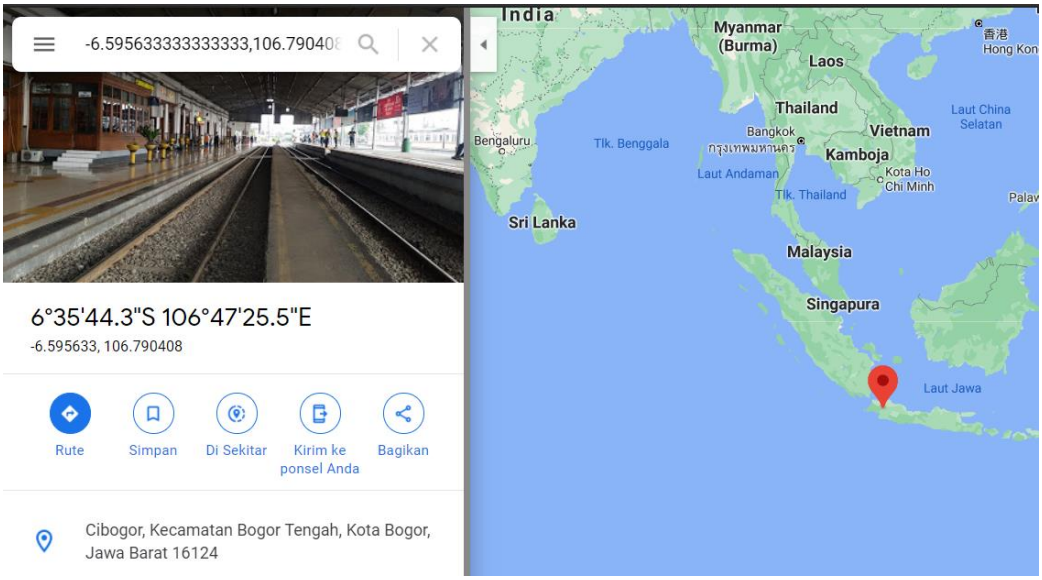
FLAG = LKSSMK28{09-22-2018}

Gambar3

Untuk soal gambar3 kita tetap menggunakan gambar yang diberikan pada soal gambar1,untuk soal gambar3 ini kita disuruh untuk mencari alamat/lokasi foto itu dibuat.

```
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Google
Profile ID                      : 75e1a6b13c34376310c8ab660632a28a
Profile Description             : sRGB IEC61966-2.1
Profile Copyright               : Copyright (c) 2016 Google Inc.
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43604 0.22249 0.01392
Green Matrix Column             : 0.38512 0.7169 0.09706
Blue Matrix Column              : 0.14305 0.06061 0.71391
Red Tone Reproduction Curve     : (Binary data 32 bytes, use -b option to extrac
t)
Chromatic Adaptation            : 1.04788 0.02292 -0.05019 0.02959 0.99048 -0.01
704 -0.00922 0.01508 0.75168
Blue Tone Reproduction Curve    : (Binary data 32 bytes, use -b option to extrac
t)
Green Tone Reproduction Curve   : (Binary data 32 bytes, use -b option to extrac
t)
Image Width                     : 2592
Image Height                    : 1944
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Aperture                        : 2.0
Image Size                      : 2592×1944
Megapixels                      : 5.0
Shutter Speed                   : 1/237
Create Date                     : 2018:09:22 09:31:08.403858
Date/Time Original              : 2018:09:22 09:31:08.403858
Modify Date                     : 2018:09:22 09:31:08.403858
GPS Altitude                    : 274 m Above Sea Level
GPS Date/Time                   : 2018:09:22 02:30:55Z
GPS Latitude                    : 6 deg 35' 44.28" S
GPS Longitude                   : 106 deg 47' 25.47" E
Focal Length                    : 2.6 mm
GPS Position                    : 6 deg 35' 44.28" S, 106 deg 47' 25.47" E
Light Value                     : 10.9
```

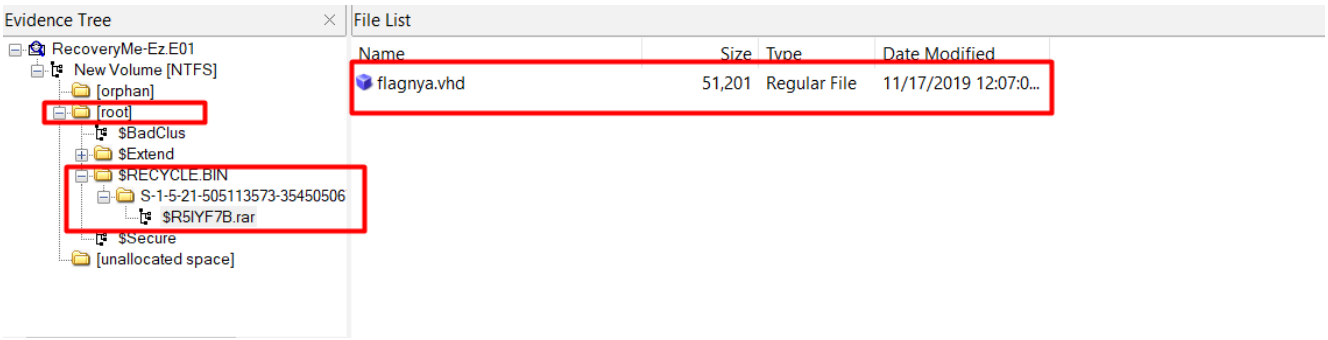
Pada gambar diatas tersebut kami menggunakan langsung perintah exiftool,lalu menemukan dimana lokasi foto itu diambil.



FLAG = LKSSMK28{Bogor}

recovery

Diberikan file berbentuk virtual,di windows yang kemungkinan di simpan di dalam sebuah file .rar



Pada gambar diatas kami mencoba menemukan file rar yang telah dihapus,dan tentu saja kami mendapatkan file tersebut,ternyata didalam file rar tersebut terdapat file flagnya.vhd

```
0ncom@kali:~/Downloads/recov$ 7z e flagnya.vhd

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.utf8,Utf16=on,HugeFiles=on,64 bits,4 CPUs Inte
l(R) Core(TM) i5-7200U CPU @ 2.50GHz (806E9),ASM,AES-NI)

Scanning the drive for archives:
1 file, 52429312 bytes (51 MiB)

Extracting archive: flagnya.vhd
--
Path = flagnya.vhd
Type = VHD
Physical Size = 52429312
Offset = 0
Created = 2019-11-16 17:03:45
Method = Fixed
Creator Application = win 6.1
Host OS = Windows
Saved State = -
ID = 4524436B9EDDCB44AF9CC5B79D5F3128
----
Size = 52428800
Packed Size = 52428800
Created = 2019-11-16 17:03:45
--
Path = flagnya.mbr
Type = MBR
Physical Size = 52428800
----
Path = 0.ntfs
Size = 49283072
File System = NTFS
Offset = 65536
Primary = +
Begin CHS = 0-2-3
End CHS = 5-254-57
--
```

Kami mencoba untuk mengdump menggunakan 7z dan diketahuilah hasil dari dump tersebut.

```
0ncom@kali:~/Downloads/recov$ ls -la
total 363384
drwxr-xr-x 7 kali kali      4096 Oct 21 10:31  .
drwxr-xr-x 9 kali kali      4096 Oct 21 10:30  ..
-rw-r--r-- 1 kali kali      2560 Nov 17  2019 '$AttrDef'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$BadClus'
-rw-r--r-- 1 kali kali      1504 Nov 17  2019 '$Bitmap'
-rw-r--r-- 1 kali kali      8192 Nov 17  2019 '$Boot'
drwx------ 2 kali kali      4096 Nov 17  2019 '$Extend'
-rw-r--r-- 1 kali kali   2097152 Nov 17  2019 '$LogFile'
-rw-r--r-- 1 kali kali    262144 Nov 17  2019 '$MFT'
-rw-r--r-- 1 kali kali      4096 Nov 17  2019 '$MFTMirr'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$ObjId'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$Quota'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$Repair'
-rw-r--r-- 1 kali kali         8 Nov 17  2019 '$Repair:$Config'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$Reparse'
drwx------ 2 kali kali      4096 Nov 17  2019 '$RmMetadata'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$Secure'
-rw-r--r-- 1 kali kali    263008 Nov 17  2019 '$Secure:$SDS'
-rw-r--r-- 1 kali kali       100 Nov 17  2019 '$Tops'
-rw-r--r-- 1 kali kali   1048576 Nov 17  2019 '$Tops:$T'
drwx------ 2 kali kali      4096 Nov 17  2019 '$Txf'
drwx------ 2 kali kali      4096 Nov 17  2019 '$TxfLog'
-rw-r--r-- 1 kali kali     65536 Nov 17  2019 '$TxfLog.blf'
-rw-r--r-- 1 kali kali   2097152 Nov 17  2019 '$TxfLogContainer00000000000000000
001'
-rw-r--r-- 1 kali kali   2097152 Nov 17  2019 '$TxfLogContainer00000000000000000
002'
-rw-r--r-- 1 kali kali    131072 Nov 17  2019 '$UpCase'
-rw-r--r-- 1 kali kali         0 Nov 17  2019 '$Volume'
-rw-r--r-- 1 kali kali  52429312 Oct 21 10:16  flagnya.vhd
-rw-r--r-- 1 kali kali        22 Nov 17  2019  flag.txt
-rw-r--r-- 1 kali kali 311544419 Nov 17  2019  RecoveryMe-Ez.flp
drwx------ 2 kali kali      4096 Oct 21 10:16 '[SYSTEM]'
```

Dan kami menemukan flag.txt

```
0ncom@kali:~/Downloads/recov$ cat ./flag.txt
flag=k0d4m-5-Br4W1Jaya0ncom@kali:~/Downloads/recov$
0ncom@kali:~/Downloads/recov$
0ncom@kali:~/Downloads/recov$
0ncom@kali:~/Downloads/recov$ md5sum flag.txt
54fd9c99c7ca8ec2c59ea8ba3c239410  flag.txt
0ncom@kali:~/Downloads/recov$
```

Lalu kami mengikuti format flag yang sudah diberikan bahwasanya isi flag adalah MD5 Dari file flag.txt tersebut dan isi dari flag.txt tersebut.

FLAG = LKSSMK28{54fd9c99c7ca8ec2c59ea8ba3c239410_ k0d4m-5-Br4W1Jaya}

Reverse

Simple Encrypt

Diberikan sebuah Enkripsi pada soal ini TEtTU01LMjh7Y mFzZTY0X0VuY3 J5cHQxMDBufQ==

```
0ncom@kali:~/Downloads/CTF_LKS2020$ echo TEtTU01LMjh7YmFzZTY0X0VuY3J5cHQxMDBufQ=
= | base64 --decode
LKSSMK28{base64_Encrypt100n}0ncom@kali:~/Downloads/CTF_LKS2020$
```

Langsung saja kami menggunakan perintah echo untuk mendecode base64 tersebut.

LKSSMK28{base64_Encrpyt100n}