

LATIHAN CYBER SECURITY

Reja_revaldy_f.

Answered

- Crypto 1
- Crypto 2
- Crypto 3
- Crypto 4
- Crypto 5
- Forensic 1
- Forensic 2
- Forensic 3
- Reverse 1
- Stego 1
- Stego 2

Unanswered

- Stego 3
- Web 1 {Unactive Link}
- Web 2 {Unactive Link}
- Web 3 {Unactive Link}

PENYELESAIAN

Crypto 1

1. Setelah saya membuka clue muncul "WTBVU19QNDRTU1cwUkQK" yang berupa bas64 lalu setelah saya decode muncul sebuah strings "Y0UR_P44SW0RD"

```
(kali㉿kali)-[~/.../Latihan/Crypto 1/Crypto 1_FILES/Crypt]
$ ls
ctf2017.png.zip  passwordmuadadidalam.txt

(kali㉿kali)-[~/.../Latihan/Crypto 1/Crypto 1_FILES/Crypt]
$ cat passwordmuadadidalam.txt
WTBVU19QNDRTU1cwUkQK

(kali㉿kali)-[~/.../Latihan/Crypto 1/Crypto 1_FILES/Crypt]
$ echo -n "WTBVU19QNDRTU1cwUkQK" | base64 --decode
Y0UR_P44SSW0RD

(kali㉿kali)-[~/.../Latihan/Crypto 1/Crypto 1_FILES/Crypt]
$
```

FLAG = {y0ur_p44sw0rd}

Crypto 2

1. Setelah membuka clue saya melakukan cipher identifier di website “<https://www.boxentriq.com/code-breaking/cipher-identifier>” terlihat enkripsi menggunakan vigenere cipher



2. Lalu saya melakukan decode vigenere cipher di situs yang sama dan saya menemukan flagnya

Results

Decoded message.

def con ctf - something like a world cup of all other competitions.mixed competitions may vary possible formats. it may be something like wargame with special time for task-based elements (like ucsb ictf).ctf games often touch on many other aspects of information security: cryptography, stego, binary analysis, reverse engineering, mobile security and others. good teams generally have strong skills and experience in all these issues.flag : idx{jangan_lupain_yang_lama_dong}

Copy

Text Options...

Not seeing the correct result? Try **Auto Solve** or use the [Cipher Identifier Tool](#).

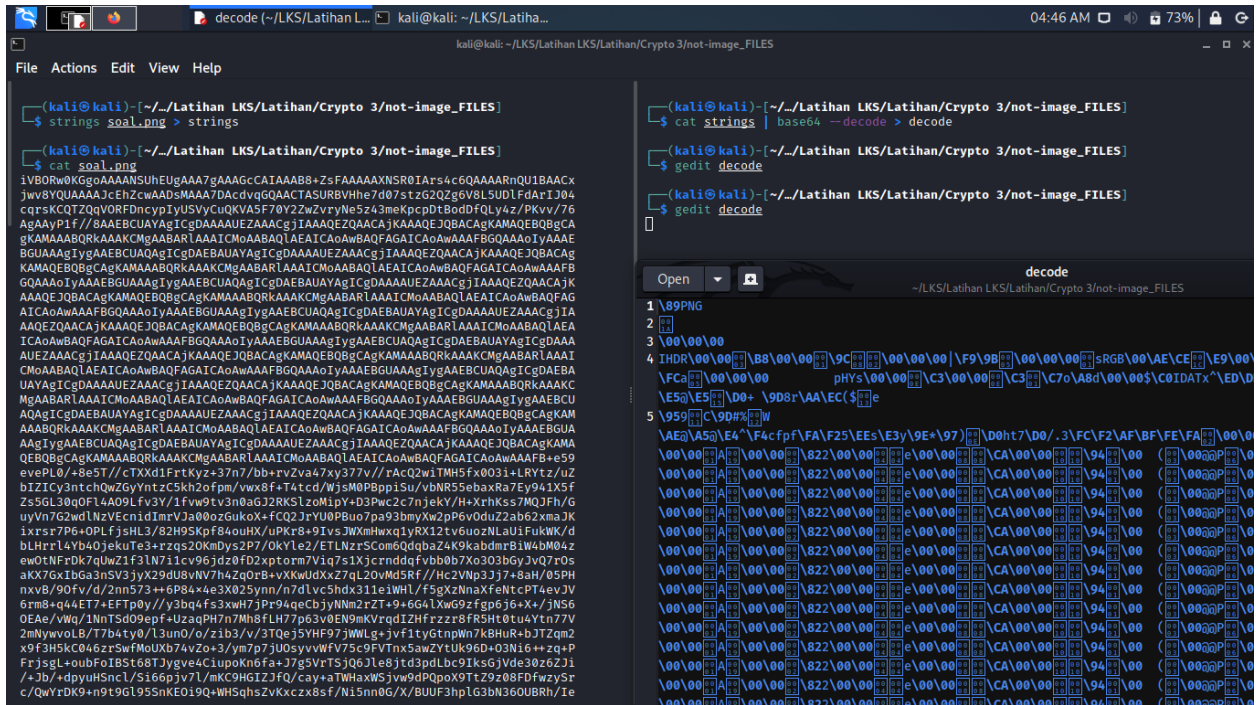
Auto Solve results

Score	Key	Text
38118	mpxyjclhm	capture the flag ctf is a special kind of information security competitions there are three common types of ctfs jeopardy attack defence and mixed jeopardy style ctfs has a couple of questions tasks in range of categories for example web forensic crypto binary or something else team can gain some points for every solved task more points for more complicated tasks usually the next task in chain can be opened only after some team solve previous task then the game time is over sum of points shows y

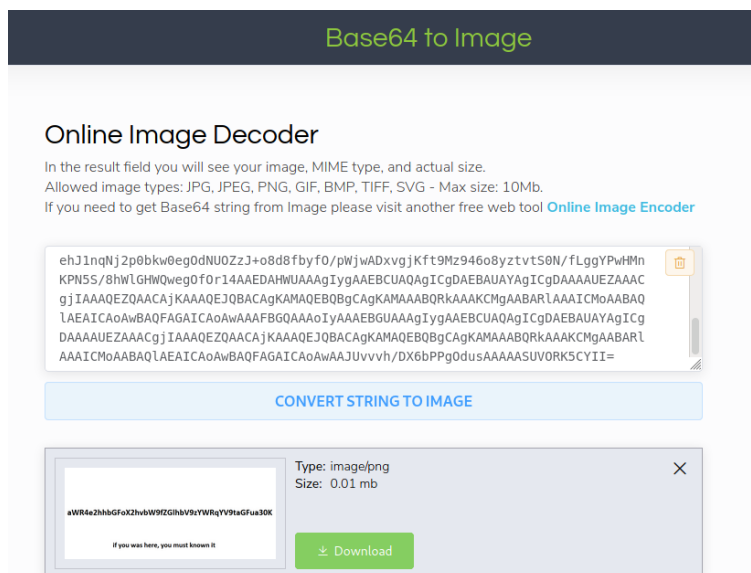
FLAG = idx{jangan_aupaen_yang_lama_dong}

Crypto 3

1. Saya melakukan strings kepada gambar lalu menemukan base64



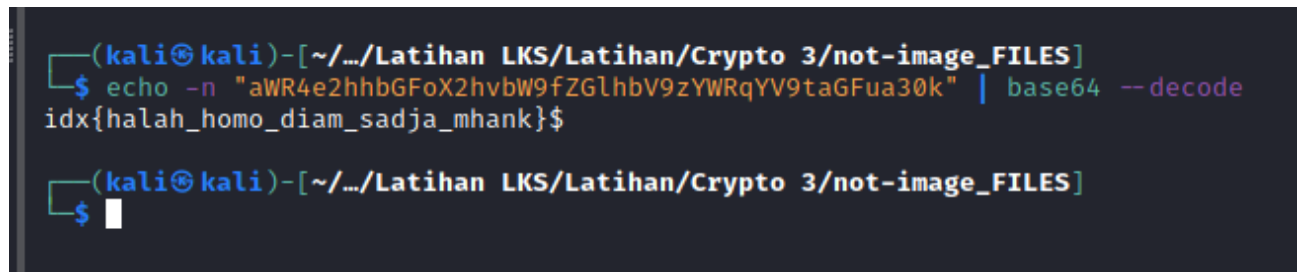
2. Lalu saya melakukan Konversi base64 ke file png



3. Dan menemukan base64 dan saya melakukan decode dan mendapatkan flagnya

aWR4e2hhbGFoX2hvbW9fZGlhbV9zYWRqYV9taGFua30K

if you was here, you must known it

A terminal window with a dark background. The prompt is (kali@kali)-[~/.../Latihan LKS/Latihan/Crypto 3/not-image_FILES]. The user enters the command: echo -n "aWR4e2hhbGFoX2hvbW9fZGlhbV9zYWRqYV9taGFua30K" | base64 --decode. The output is: idx{halah_homo_diam_sadja_mhank}\$. The user then enters a new command, and the prompt returns.

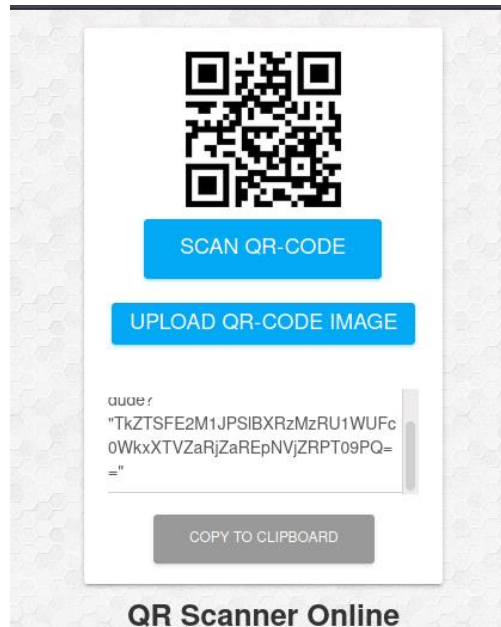
```
(kali@kali)-[~/.../Latihan LKS/Latihan/Crypto 3/not-image_FILES]
$ echo -n "aWR4e2hhbGFoX2hvbW9fZGlhbV9zYWRqYV9taGFua30K" | base64 --decode
idx{halah_homo_diam_sadja_mhank}$

(kali@kali)-[~/.../Latihan LKS/Latihan/Crypto 3/not-image_FILES]
$
```

FLAG = idx{halah_homo_diam_sadja_mhank}

Crypto 4

1. Diberikan qr code lalu saya scan dan muncul base64



2. Lalu saya melakukan decode dan muncul hash berupa base32 dan saya melakukan decode lagi dan muncul flag

```
kali@kali: ~/LKS/Latihan LKS/Latihan/Crypto 4/ojo-menteleng_FILES
File Actions Edit View Help

(kali@kali)-[~/LKS/Latihan LKS/Latihan/Crypto 4/ojo-menteleng_FILES]
$ echo -n "TkZTSFE2M1JPSlBXRzMzRU1WUFc0WkxXTVZaRjZaREpNVjZRPT09PQ==" | base64 --decode
NFSHQ63R0JPWG33EMVPW4ZLWMVZF6ZDJMV6Q==

(kali@kali)-[~/LKS/Latihan LKS/Latihan/Crypto 4/ojo-menteleng_FILES]
$ echo -n "NFSHQ63R0JPWG33EMVPW4ZLWMVZF6ZDJMV6Q==" | base32 --decode
idx{qr_code_never_die}

(kali@kali)-[~/LKS/Latihan LKS/Latihan/Crypto 4/ojo-menteleng_FILES]
$
```

FLAG = idx{qr_code_never_die}

Crypto 5

1. Diberikan sebuah clue lalu ditemukan strings dan saya melakukan cipher identifier di ["https://www.boxentriq.com/code-breaking/cipher-identifier"](https://www.boxentriq.com/code-breaking/cipher-identifier) dan muncul cipher yang digunakan berupa "Monoalphabetic substitution" dan saya melakukan decode di website yang sama dan muncul flag nya

BOXENTRIQ

HOME ABOUT CODE BREAKING FAQ HALL OF FAME CONTACT

G1 smknurgld, t ftsibp gq tly qigjjba smknurbp bxnbrp rftr uqbq rfbgp rbsflgstj ilmwjbadb rm mvbpsmkb t npmejbk. Wfgjb "ftsibp" stl pbcbbp rm tly smknurbp npmdptkbbp, rfb rbpk ftq ebsmkb tqmsgtrba gl nmnujtp sujrupb wgrf t "qbsupgry ftsibp", qmkbmlb wfm, wgrf rfbgp rbsflgstj ilmwjbadb, uqbq eudq mp bxnjmgrq rm epbti glrm smknurbp qyqrbkq. Cjtd gq : gax{ktqrbp_mc_spyrnm_fbpb}

Analyze Text Copy Paste Text Options...

Note: To get accurate results, your ciphertext should be at least 25 characters long.

Analysis Results

G1 smknurgld, t ftsibp gq tly qigjjba smknurbp bxnbrp rftr uqbq rfbgp rbsflgstj ilmwjbadb rm mvbpsmk...

Your ciphertext is likely of this type:

[Monoalphabetic Substitution Cipher \(click to read more\)](#)

BOXENTRIQ

HOME ABOUT CODE BREAKING FAQ HALL OF FAME CONTACT

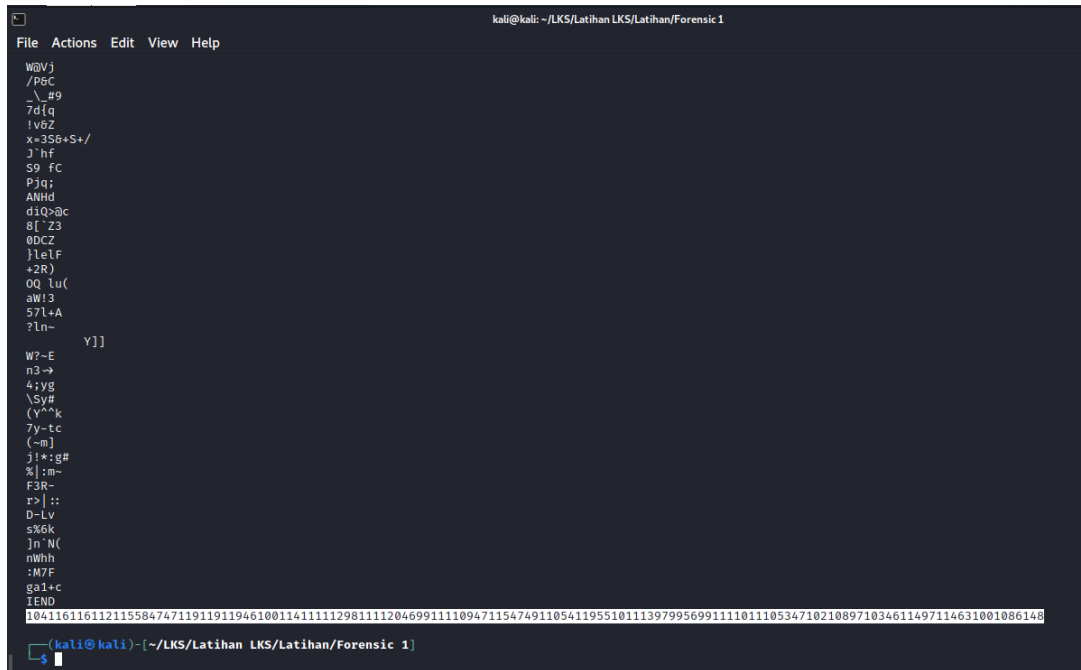
Auto Solve Results

Score	Text
35364	in computing a hacker is any skilled computer expert that uses their technical knowledge to overcome a problem while hacker can refer to any computer programmer the term has become associated in popular culture with a security hacker someone who with their technical knowledge uses bugs or exploits to break into computer systems flag is idx master of crypto here
14376	im talkupimg o rothen is ony shifted talkupen exkxnp prop uses prein petrmitof hmcdfedge pa aventale o knabfel crife rothen tom newen pa omy talkupen knagnollen pre penl ros betale ossatioped im kakufon tufpune cipr o setunipy rothen saleame era cipr prein petrmitof hmcdfedge uses bugs an exkfaips pa bneoh impa talkupen syspels wfog is idx lospen aw tnykpa rene
10787	un rewschund a mariot up any piullok rewschot ovsoth hmah cpop hmout hormnural ineblokdo he exotrewo a steflow bmuldo mariot ran togot he any rewschot stedtaawot hmo hotw map forewo apperuahok un sesclat relcto buhm a portuhy mariot pewoeno bme buhm hmout hormnural ineblokdo cpop fdcp et ovsleuhp he ftoai unhe rewschot pyphowp glad up ukv waphot eg rtysho moto
10602	at unmkpiaty o rouged as oth sgallew unmkpied evkedi iroi pses iread ieurtaul gtnflewy in nzedunne o kdnblem frale rouged uot deced in oth unmkpied kdnydommed ire iedm ros beunne ossnuaoiew at knkplod uplipde fair o seupdaih rouged snmente frn fair iread ieurtaul gtnflewy pses bpys nd evklnais in bdeog atin unmkpied shsiems cloy as awv mosied nc udhkin rede
9954	my gatiblmyp u oughes mr uyf rhmnex gatibles eviesl lou brer loems legoyngun hyawnexpe la acesgate u isadnet womne oughes guy sekas la uuf gariblee isantrres loe leet our degate nreanmuley mw isihone abalhee umlo u roehemlfouahoe rateato uoa umlo loeme loetomun

FLAG = idx{master_of_crypto_here}

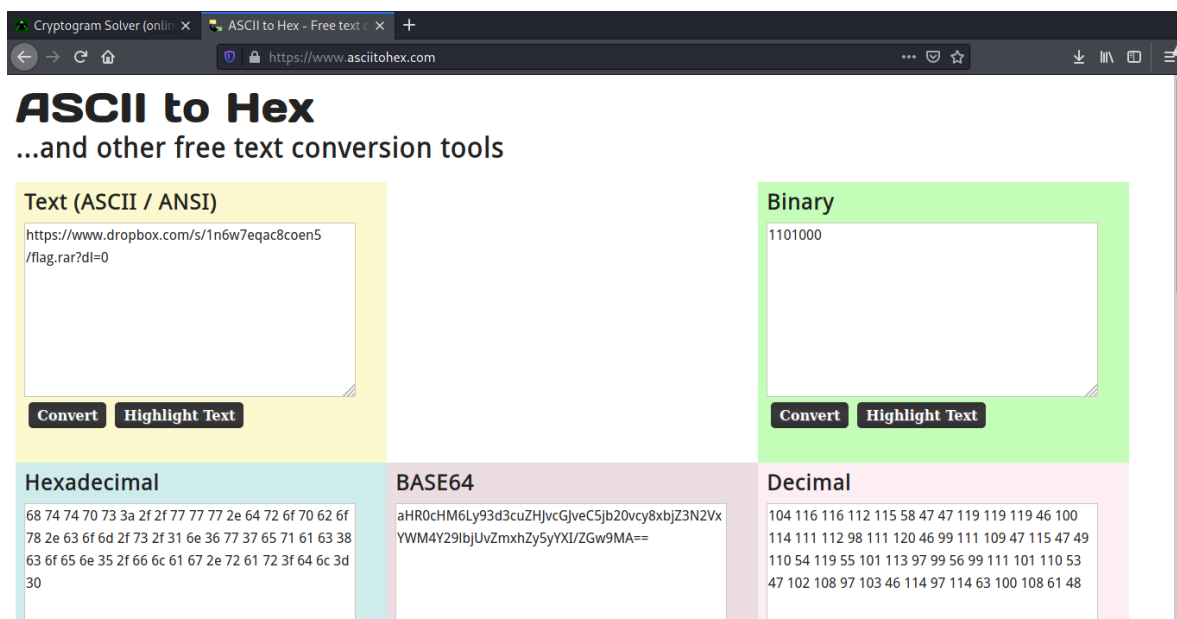
Forensic 1

1. Saya melakukan strings di gambar lalu menemukan decimal di akhir



```
kali@kali: ~/LKS/Latihan LKS/Latihan/Forensic 1
File Actions Edit View Help
W@Vj
/P6C
\_#9
7d{q
!v0Z
x=356+S+/
J`hf
S9 fC
Piq;
ANhd
diQ>@c
8[`Z3
00CZ
}lelF
+2R)
00 Lu(
aWl3
57l+A
7ln~
Y]]
W7-E
n3->
4:yg
\5y#
(y~^k
7y~tc
(-m]
j!*:g#
%|:m~
F3R-
r>|::
D~Lv
s%6k
Jn`N(
mWhh
:W7F
g3l+c
IEND
10411611611211558474711911911946100114111129811112046991111094711547491105411955101113979956991111011105347102108971034611497114631001086148
(kali@kali)~-[~/LKS/Latihan LKS/Latihan/Forensic 1]
```

2. Lalu saya melakukan decode di “asciitohex.com” dan muncul link yang berupa folder flag



- ```
kali@kali: ~/LKS/Latihan... 05:11 AM 89%
File Actions Edit View Help
└─$ 1;2c1;2c1;2c1;2c1;2c1;2c1;2cclear 1 ⊕

(kali@kali)-[~/LKS/Latihan LKS/Latihan/Forensic 1/flag]
└─$ cat decode 130 × 1 ⊕
❖❖❖❖JFIF❖❖❖❖8ExifMM❖❖❖❖❖❖❖❖idx{Smithys_werben_jegen_man_jensen}idx{Smithys_werben_jegen_man_jense
n_mithys_werben_jegen_man_jensen}
❖❖❖❖❖❖❖❖idx{Smithys_werben_jegen_man_jensen}idx{Smithys_werben_jegen_man_jensen}❖❖❖❖
1

http://ns.adobe.com/xap/1.0/?xpacket begin=' id="WEMOMpCehiHzeSzNtczk9d">
<x:xmpmeta xmlns:x="adobe:namespaces:"><rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:
Description rdf:about="uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.
1/"><dc:title><rdf:Alt xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:li xml:lang="x-default
">idx{Smithys_werben_jegen_man_jensen}</rdf:li></rdf:Alt>
</dc:title><dc:description><rdf:Alt xmlns:rdf="http://www.w3.org/1999/02/22-rdf-sy
ntax-ns#"><rdf:li xml:lang="x-default">idx{Smithys_werben_jegen_man_jensen}</rdf:li></rdf:Alt>
</dc:description></rdf:Description><rdf:Description rdf:about="uuid:faf5bdd5-ba3d-
11da-ad31-d33d75182f1b" xmlns:dc="http://purl.org/dc/elements/1.1/" /></rdf:RDF></x:xmpmeta>

⋮

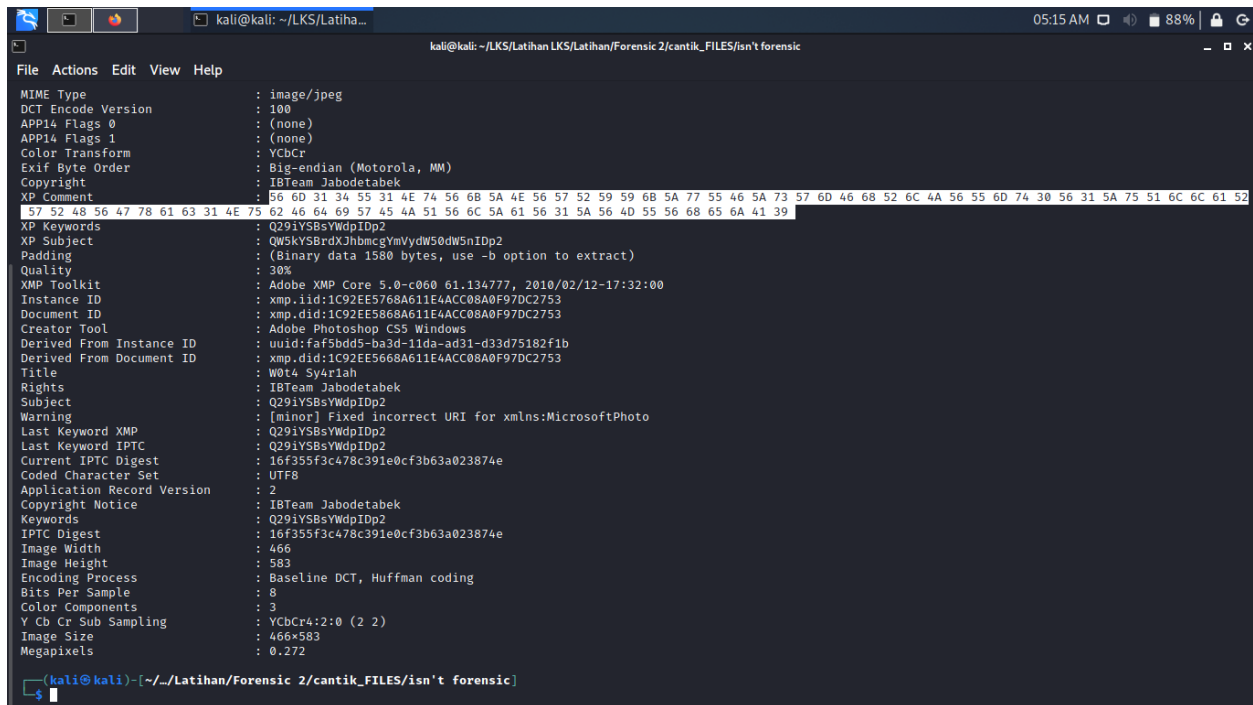
<?xpacket end="w"?>❖❖❖

"##! %*5-%'2(.7/279<<<$-BFA:F5; <9❖❖❖
```

```
FLAG = idx{Sm1thys_werben_jegen_man_jensen}
```

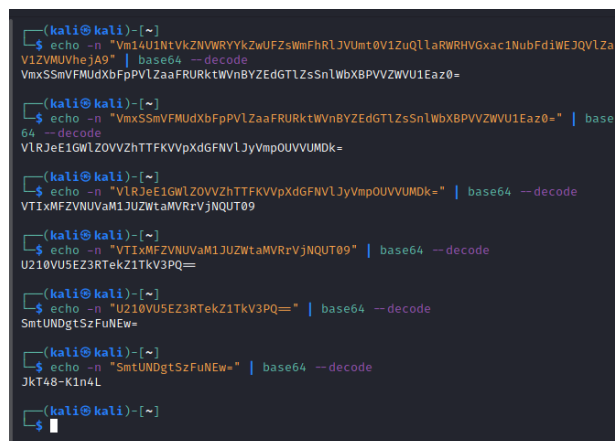
## Forensic 2

1. Diberikan png, lalu saya menggunakan exiftool dan menemukan xp comment yang saya asumsikan hexadecimal dan saya conversikan ke ascii



```
kali@kali: ~/LKS/Latiha...
kali@kali: ~/LKS/Latihan LKS/Latihan/Forensic 2/cantik_FILES/isn't forensic
File Actions Edit View Help
MIME Type : image/jpeg
DCT Encode Version : 100
APP14 Flags 0 : (none)
APP14 Flags 1 : (none)
Color Transform : YCbCr
Exif Byte Order : Big-endian (Motorola, MM)
Copyright : IBTeam Jabodetabek
XP Comment : 56 60 31 34 55 31 4E 74 56 6B 5A 4E 56 57 52 59 59 6B 5A 77 55 46 5A 73 57 6D 46 68 52 6C 4A 56 55 6D 74 30 56 31 5A 75 51 6C 6C 61 52
XP Keywords : Q29iYSBsYWdpIDp2
XP Subject : QW5kYSBrdXJhbmcyYmVydW50dW5nIDp2
Padding : (Binary data 1580 bytes, use -b option to extract)
Quality : 30%
XMP Toolkit : Adobe XMP Core 5.0-c060 61.134777, 2010/02/12-17:32:00
Instance ID : xmp:iid:1C92EE5768A611E4ACC08A0F97DC2753
Document ID : xmp:did:1C92EE5868A611E4ACC08A0F97DC2753
Creator Tool : Adobe Photoshop CS5 Windows
Derived From Instance ID : uuid:fa5bdd5-ba3d-11da-ad31-d33d75182f1b
Derived From Document ID : xmp:did:1C92EE5668A611E4ACC08A0F97DC2753
Title : W0t4 Sy4r1ah
Rights : IBTeam Jabodetabek
Subject : Q29iYSBsYWdpIDp2
Warning : [minor] Fixed incorrect URI for xmlns:MicrosoftPhoto
Last Keyword XMP : Q29iYSBsYWdpIDp2
Last Keyword IPTC : Q29iYSBsYWdpIDp2
Current IPTC Digest : 16f355f3c478c391e0cf3b63a023874e
Coded Character Set : UTF8
Application Record Version : 2
Copyright Notice : IBTeam Jabodetabek
Keywords : Q29iYSBsYWdpIDp2
IPTC Digest : 16f355f3c478c391e0cf3b63a023874e
Image Width : 466
Image Height : 583
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size : 466x583
Megapixels : 0.272
(kali@kali)-[~/LKS/Latihan/Forensic 2/cantik_FILES/isn't forensic]
```

2. Dan saya menemukan hash base64 lalu saya conversikan lagi dan menemukan base64 dan sampai saya menemukan flag nya



```
(kali@kali)-[~]
$ echo -n "Vm14U1NtVkdWVWRYkZwUfZsWmFhRLJVUmt0V1ZuQllaRWRHVgxac1NubFdiWEJQVLZa
V1ZVMUvhejA9" | base64 --decode
VmXSSmVFMudXbFpPVLZaaFRURktWVnBYZEdGTLZsSnLWbXBPVZWVU1Eaz0=

(kali@kali)-[~]
$ echo -n "VmXSSmVFMudXbFpPVLZaaFRURktWVnBYZEdGTLZsSnLWbXBPVZWVU1Eaz0=" | base
64 --decode
VLRJeE1GWLZ0VVZhTTFKVvpXdGfNVLJyVmpOUVVUMDK=

(kali@kali)-[~]
$ echo -n "VLRJeE1GWLZ0VVZhTTFKVvpXdGfNVLJyVmpOUVVUMDK=" | base64 --decode
VTIXMFZVNUVaM1JUZWtaMVRrVjNQUT09

(kali@kali)-[~]
$ echo -n "VTIXMFZVNUVaM1JUZWtaMVRrVjNQUT09" | base64 --decode
U210VU5EZ3RtekZ1TKv3PQ==

(kali@kali)-[~]
$ echo -n "U210VU5EZ3RtekZ1TKv3PQ==" | base64 --decode
SmtUNDgtSzFuNEw=

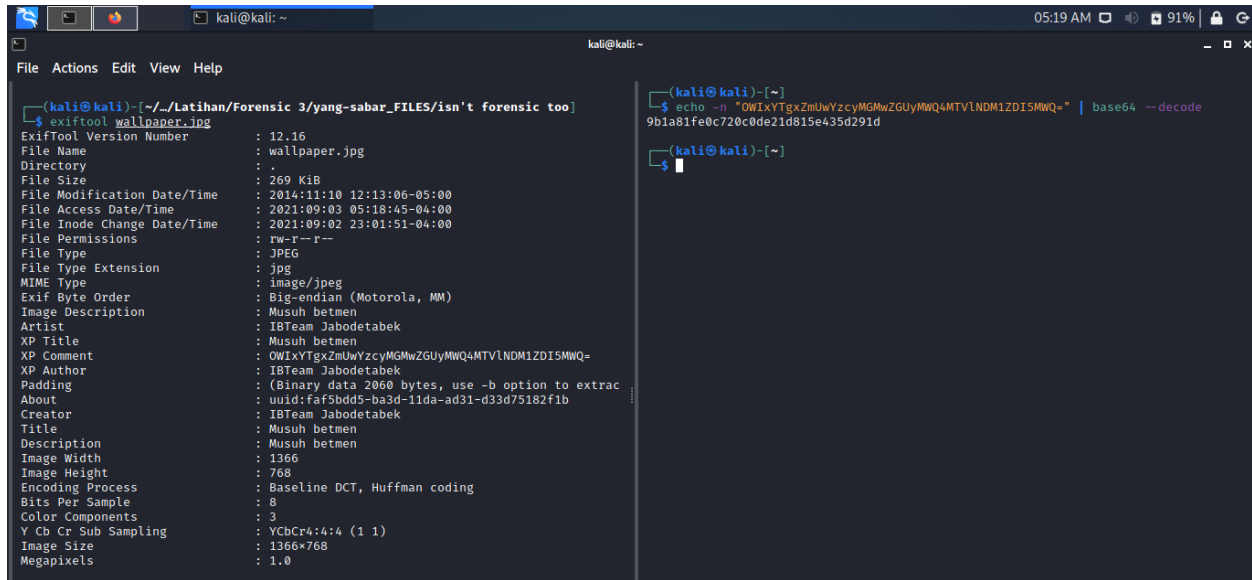
(kali@kali)-[~]
$ echo -n "SmtUNDgtSzFuNEw=" | base64 --decode
JKT48-K1n4L

(kali@kali)-[~]
$
```

FLAG = {JkT48-K1n4L}

## Forensic 3

1. Diberikan gambar png lalu saya menggunakan exiftool dan menemukan xp comment yang berupa base64 dan saya melakukan decode dan menemukan md5

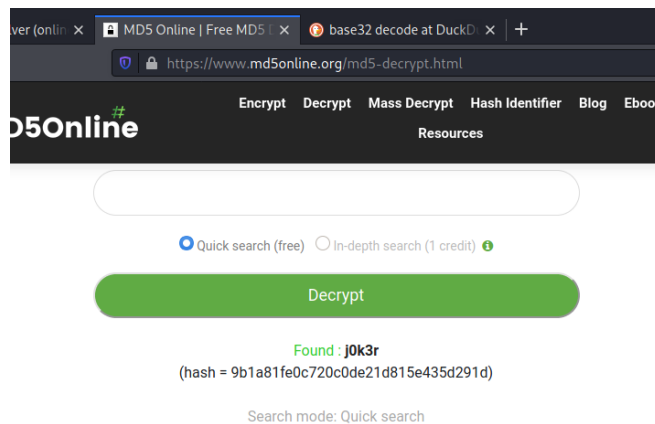


```
(kali@kali)-[~/Latihan/Forensic 3/yang-sabar_FILES/Isn't forensic too]
$ exiftool wallpaper.jpg
ExifTool Version Number : 12.16
File Name : wallpaper.jpg
Directory : .
File Size : 269 KiB
File Modification Date/Time : 2014:11:10 12:13:06-05:00
File Access Date/Time : 2021:09:03 05:18:45-04:00
File Inode Change Date/Time : 2021:09:02 23:01:51-04:00
File Permissions : rw-r--r--
File Type : JPEG
File Type Extension : jpg
MIME Type : image/jpeg
Exif Byte Order : Big-endian (Motorola, MM)
Image Description :
Artist : I8Team Jabodetabek
XP Title : Musuh betmen
XP Comment : OWIXYtgxZmUwYzcyMGhwZGUyMmQ4MTVlNDM1ZDI5MmQ=
XP Author : I8Team Jabodetabek
Padding : (Binary data 2060 bytes, use -b option to extract)
About : uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator : I8Team Jabodetabek
Title : Musuh betmen
Description : Musuh betmen
Image Width : 1366
Image Height : 768
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
Y Cb Cr Sub Sampling : YCbCr4:4:4 (1 1)
Image Size : 1366x768
Megapixels : 1.0

(kali@kali)-[~]
$ echo -n "OWIXYtgxZmUwYzcyMGhwZGUyMmQ4MTVlNDM1ZDI5MmQ=" | base64 --decode
9b1a81fe0c720c0de21d815e435d291d

(kali@kali)-[~]
$
```

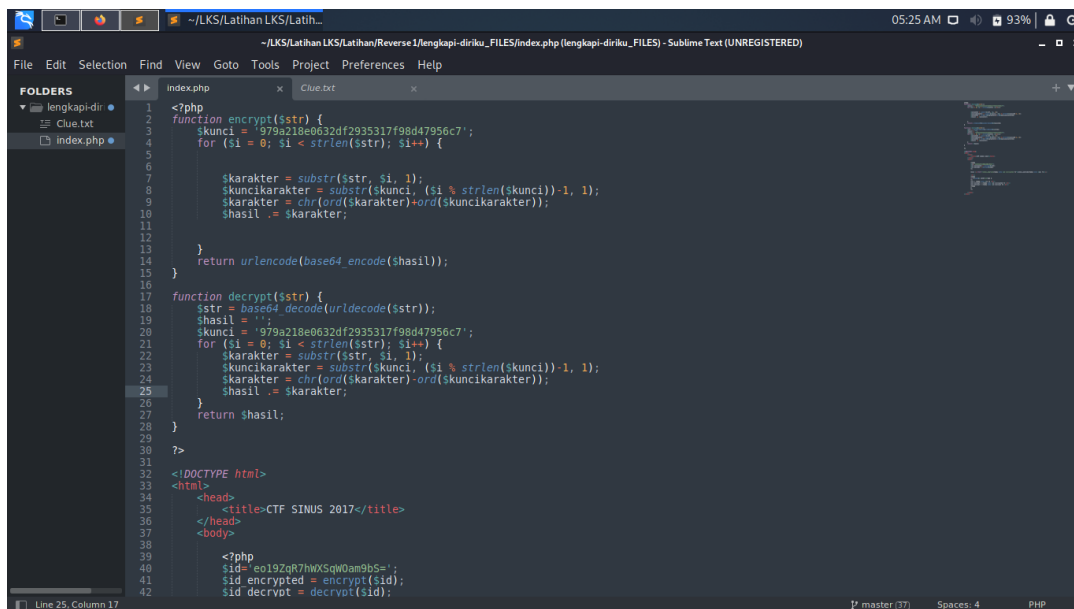
2. Lalu saya melakukan decode md5 dan muncul flag



FLAG = {j0k3r}

## Reverse 1

1. Diberikan index php dan clue berupa string, di index php diberikan function encrypt dan decrypt, lalu saya melengkapi function decrypt yang belum selesai dengan cara mengikuti function encrypt diatas dan melakukan decode di function decrypt



```
<?php
function encrypt($sstr) {
 $skunci = '979a218e0632df2935317f98d47956c7';
 for ($i = 0; $i < strlen($sstr); $i++) {

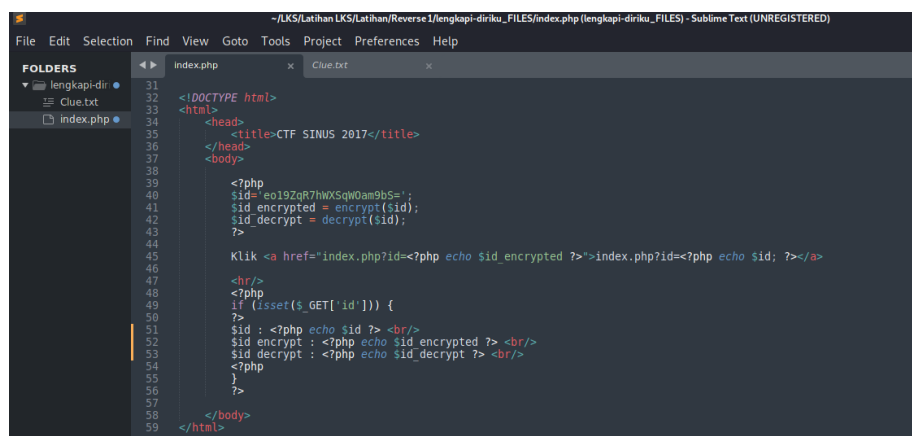
 $karakter = substr($sstr, $i, 1);
 $skunkikarakter = substr($skunci, ($i % strlen($skunci))-1, 1);
 $karakter = chr(ord($karakter)+ord($skunkikarakter));
 $hasil .= $karakter;
 }
 return urlencode(base64_encode($hasil));
}

function decrypt($sstr) {
 $sstr = base64_decode(urldecode($sstr));
 $hasil = '';
 $skunci = '979a218e0632df2935317f98d47956c7';
 for ($i = 0; $i < strlen($sstr); $i++) {
 $karakter = substr($sstr, $i, 1);
 $skunkikarakter = substr($skunci, ($i % strlen($skunci))-1, 1);
 $karakter = chr(ord($karakter)-ord($skunkikarakter));
 $hasil .= $karakter;
 }
 return $hasil;
}
?>

<!DOCTYPE html>
<html>
<head>
<title>CTF SINUS 2017</title>
</head>
<body>

<?php
$id = e019ZqR7hWXSqW0am9b5=';
$id encrypted = encrypt($id);
$id decrypt = decrypt($id);
?>
```

2. Lalu saya memasukan id dengan text yang diberikan di clue lalu saya panggil function decrypt yang berisi id dan muncul flagnya



```
<?php
function encrypt($sstr) {
 $skunci = '979a218e0632df2935317f98d47956c7';
 for ($i = 0; $i < strlen($sstr); $i++) {

 $karakter = substr($sstr, $i, 1);
 $skunkikarakter = substr($skunci, ($i % strlen($skunci))-1, 1);
 $karakter = chr(ord($karakter)+ord($skunkikarakter));
 $hasil .= $karakter;
 }
 return urlencode(base64_encode($hasil));
}

function decrypt($sstr) {
 $sstr = base64_decode(urldecode($sstr));
 $hasil = '';
 $skunci = '979a218e0632df2935317f98d47956c7';
 for ($i = 0; $i < strlen($sstr); $i++) {
 $karakter = substr($sstr, $i, 1);
 $skunkikarakter = substr($skunci, ($i % strlen($skunci))-1, 1);
 $karakter = chr(ord($karakter)-ord($skunkikarakter));
 $hasil .= $karakter;
 }
 return $hasil;
}
?>

<!DOCTYPE html>
<html>
<head>
<title>CTF SINUS 2017</title>
</head>
<body>

<?php
$id = e019ZqR7hWXSqW0am9b5=';
$id encrypted = encrypt($id);
$id decrypt = decrypt($id);
?>

Klik <a href='index.php?id=<?php echo $id_encrypted ?>'>index.php?id=<?php echo $id; ?>

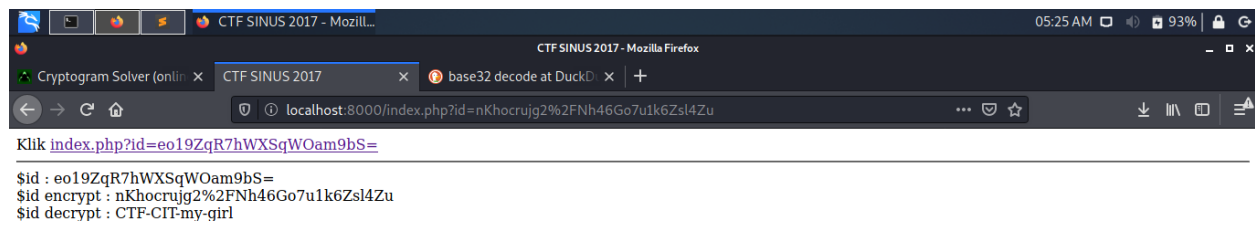
<hr/>
<?php
if (isset($_GET['id'])) {
 ?>
 $id : <?php echo $id ?>

 $id encrypt : <?php echo $id encrypted ?>

 $id decrypt : <?php echo $id decrypt ?>

 <?php
 }
?>


</body>
</html>
```



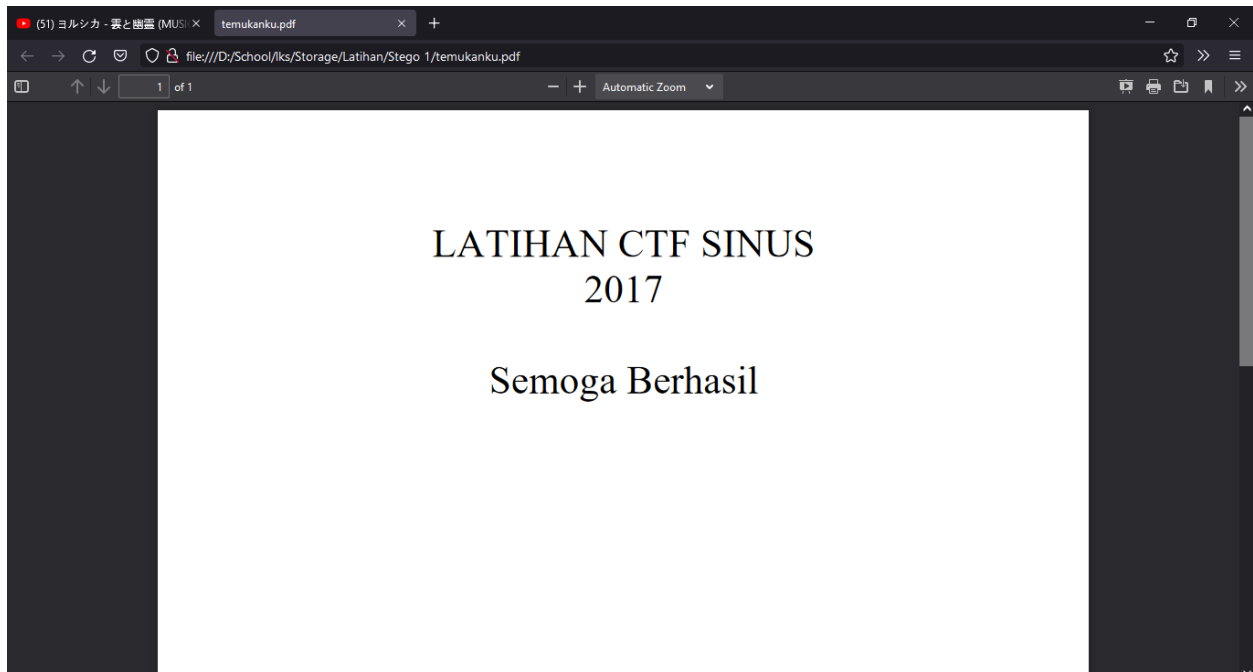
FLAG = {CTF-CIT-my-girl}

## Stego 1

1. Diberikan file dengan nama temukankupdf

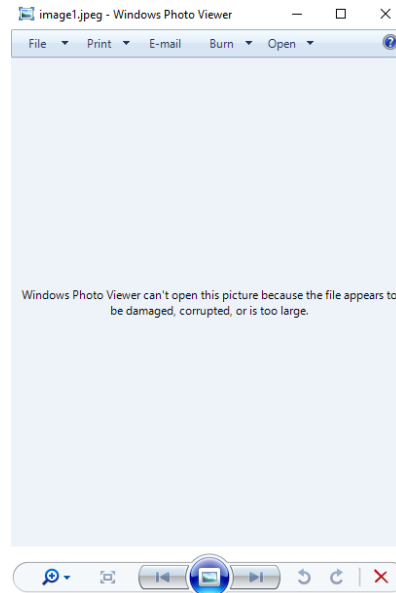
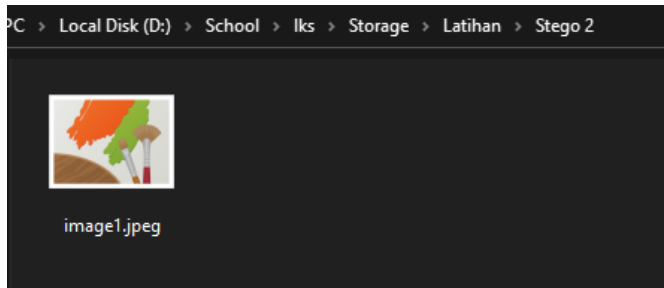
Name	Date modified	Type	Size
 temukankupdf	12/9/2017 10:37 PM	File	7 KB

2. Lalu saya menambahkan extension .pdf di file tersebut  
Setelah saya buka file yang sudah saya tambahkan  
extension .pdf maka muncul



## Stego 2

1. Diberikan file gambar dan setelah saya buka gambar tersebut tidak terlihat apa apa atau corrupt



2. Lalu saya mencoba membuka file gambar menggunakan notepad maka muncul seperti ini, lalu saya mencoba mengubah extension nya ke wav karena ada tulisan wave di file tersebut (saya mencoba mencari riff wave di internet dan menemukan file tersebut adalah wav)





3. Lalu setelah saya ubah maka saya menggunakan audacity untuk mendengarkan nya, setelah saya dengarkan saya mendengar suara yang sangat cepat dan setelah saya putar dengan kecepatan rendah saya masih belum mendengar dengan jelas suara nya

