

**APTIKOM**  
**Nusantara Cyber Security 2025**

# **WRITE UP**

Sabtu, 20 September 2025

**Nama Perguruan Tinggi** : UPN “Veteran” Yogyakarta  
**Nama Tim** : Soft Spoken  
**Ketua Tim** : Muhammad Luqmaan  
**Anggota** :  
1. Muhamad Akbar Riziq  
2. Muhammad Adel Harits  
**E-mail Tim** : Muhammad Luqmaan ([mluqmaan22@gmail.com](mailto:mluqmaan22@gmail.com))  
Muhamad Akbar Riziq ([akbarriziq348@gmail.com](mailto:akbarriziq348@gmail.com))  
Muhammad Adel Harits ([adel.harits18@gmail.com](mailto:adel.harits18@gmail.com))

**APTIKOM**  
**Nusantara Cyber Security 2025**

**Daftar isi**

**[Easy]**

- 3 ..... **Seorang tokoh nasional meninggalkan pesan yang disandikan**  
4 ..... **Looking for something**  
5 ..... **Jangan iseng baca chat teman**

**[Medium]**

- 7 ..... **Pesan dari Pejuang**  
8 ..... **Everything has changed**

# **APTIKOM**

## **Nusantara Cyber Security 2025**

### **1. Soal No 1 (Seorang tokoh nasional meninggalkan pesan yang disandikan)**

**Flag :**

ncs(semangat\_kebangsaan}

**Deskripsi :**

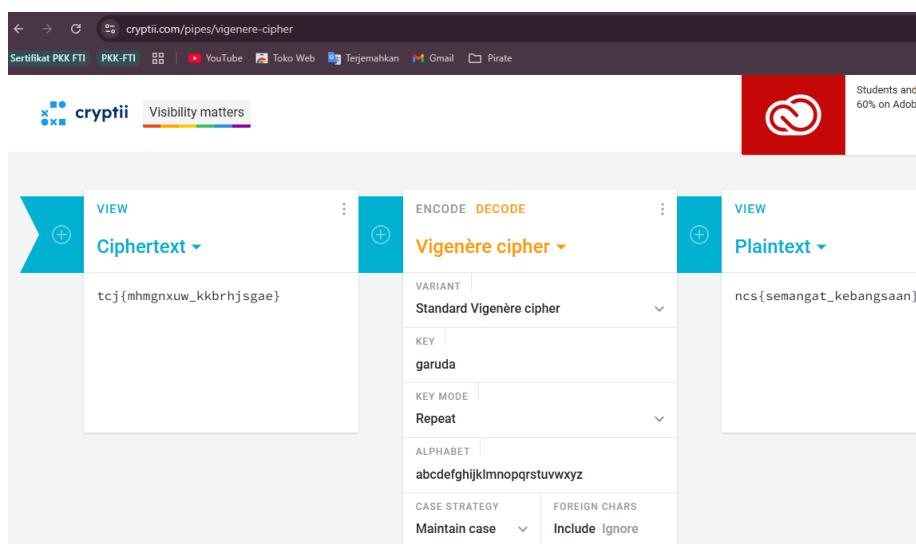
Seorang tokoh nasional meninggalkan pesan yang disandikan menggunakan metode Vigenère Cipher. Berikut adalah pesan yang ditemukan:

**tcj{mhmgnxuw\_kkbrhjsgae}**

Kunci yang digunakan untuk mengenkripsi pesan adalah: Lambang Negara

**Solusi :**

Pada soal sudah dijelaskan kalau algoritma yang digunakan adalah vigenere cipher dengan kunci lambang negara. Kita bisa menggunakan website <https://cryptii.com/pipes/vigenere-cipher> untuk memecahkan sandi tersebut dengan memasukkan ciphertext dari soal dan kunci garuda yang merupakan lambang negara indonesia.



The screenshot shows the Cryptii website interface for decoding a Vigenère cipher. The URL in the address bar is cryptii.com/pipes/vigenere-cipher. The main interface has three main sections: Ciphertext (left), Variant (center), and Plaintext (right). The Ciphertext section contains the input 'tcj{mhmgnxuw\_kkbrhjsgae}'. The Variant section is set to 'Standard Vigenère cipher'. The Key section shows 'garuda' as the key. The resulting Plaintext is 'ncs(semangat\_kebangsaan)'.

Hasilnya flagnya muncul yaitu **ncs(semangat\_kebangsaan}**

# APTIKOM

## Nusantara Cyber Security 2025

### 2. Soal No 2 (Looking for something)

**Flag:**

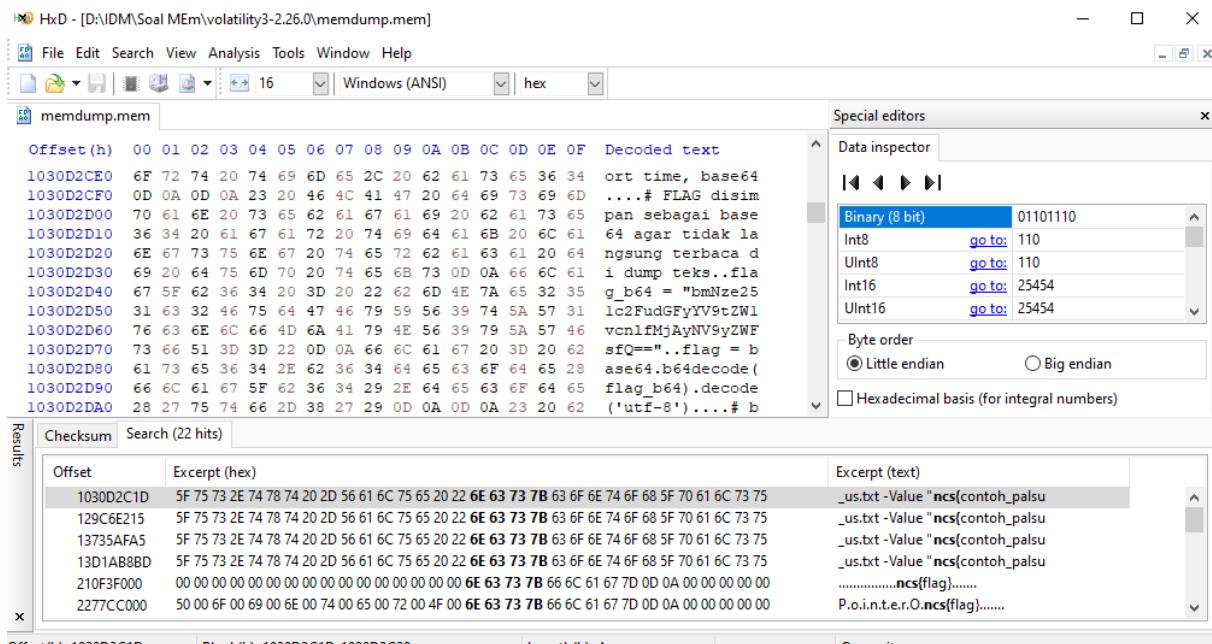
ncs{nusantara\_memory\_2025\_real}

**Deskripsi :**

Silahkan Download file berikut :  
<https://drive.google.com/file/d/19tg1IHIdYFaj9f6jMMLpb4PFxpqQERNr/view?usp=sharing>

**Solusi:**

Pada file 7z yang diberikan, bisa langsung di unzip dan akan mendapatkan file yaitu memdump.mem. Lalu gunakan hxd untuk melihat isi pada file tersebut. Karna penasaran, langsung search apakah ada string dengan format ncs{}, setelah dicari ternyata terdapat string dengan format ncs yang palsu untuk menipu.



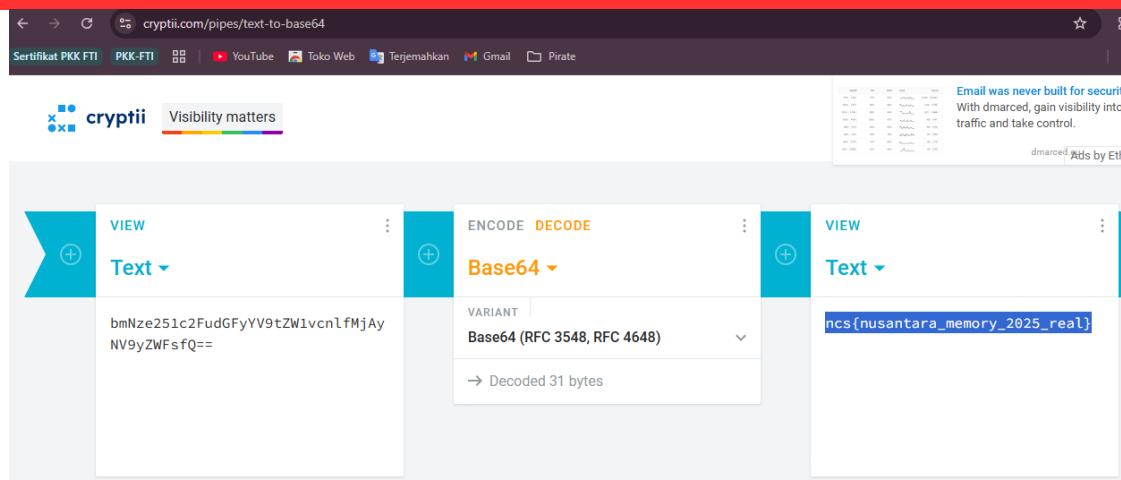
The screenshot shows the HxD Hex Editor interface. The main window displays the memory dump file 'memdump.mem'. The 'Data inspector' panel on the right shows the binary representation of the string 'ncs{contoh\_palsu}', which is encoded in base64 as 'bmNze251c2FudGFyYV9tZW1vcm1lMFjaYNV9yZWFsfQ=='. The 'Results' panel at the bottom shows a list of 22 hits for the string 'ncs{contoh\_palsu}'.

Offset	Excerpt (hex)	Excerpt (text)
1030D2C1D	5F 75 73 2E 74 78 74 20 2D 56 61 6C 75 65 20 22	_us.txt -Value "ncs{contoh_palsu"
129C6E215	5F 75 73 2E 74 78 74 20 2D 56 61 6C 75 65 20 22	_us.txt -Value "ncs{contoh_palsu"
13735AFA5	5F 75 73 2E 74 78 74 20 2D 56 61 6C 75 65 20 22	_us.txt -Value "ncs{contoh_palsu"
13D1AB8BD	5F 75 73 2E 74 78 74 20 2D 56 61 6C 75 65 20 22	_us.txt -Value "ncs{contoh_palsu"
210F3F000	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....ncs{flag}.....
2277CC000	50 00 6F 00 69 00 6E 00 74 00 65 00 72 00 4F 00	P.o.i.n.t.e.r.O.ncs{flag}.....

Pada hxd tersebut terdapat tulisan jika flag disembunyikan menjadi base64 agar sulit untuk diketahui. Akhirnya menggunakan website <https://cryptii.com/pipes/text-to-base64> untuk mendecrypt base64 tersebut menjadi string seperti biasa

# APTIKOM

## Nusantara Cyber Security 2025



The screenshot shows a web-based tool for encoding and decoding data. In the center, there is a 'DECODE' section set to 'Base64'. Below it, the text 'bmNze251c2FudGFyVV9tZW1vcnlfMjAyNV9yZWfsfQ==' is being decoded. A message box indicates that 31 bytes have been decoded. To the right, the resulting text 'ncs{[REDACTED]}' is shown.

Dan hasilnya flagnya terbaca yaitu **ncs{[REDACTED]}**

### 3. Soal No 3 (Jangan iseng baca chat teman)

**Flag:**

ncs{SQL-oH\_sql-1974}

**Deskripsi:**

Tanpa sengaja aku melihat backup database di laptop teman, aku iseng saja mencoba melihat apa isi didalamnya, aku penasaran dengan isi chat teman-teman ku, aku yakin disana ada info flag yang kubutuhkan.

**Solusi:**

Dari format file `chat_backup.db` saya langsung mencoba sqlite untuk mencoba melihat isi file tersebut, ada banyak message dengan format yang tampak terenkripsi. Beberapa terlihat jelas jika itu adalah format base64. Namun saat dekripsi dilakukan, ada yang tidak berhasil menjadi string jelas yang kemudian dilakukan dekripsi lagi, tetapi malah ada `ncs{n0t-th1s_chAt}` yang di mana itu bukanlah flagnya. Kita sangat kebingungan hingga akhirnya memutuskan untuk membuka hint dan mendapatkan hint `0x42`. Saya terpikirkan jika itu merupakan operasi xor dengan kunci `0x42`. Kemudian saya membuat script yang isinya untuk 'setelah di-decode sekali dengan base64'.

# APTIKOM

## Nusantara Cyber Security 2025

### Jawaban:

```

❸ solve.py > ⌂ extract_the_flag
 1  import base64
 2  import re
 3
 4  def extract_the_flag():
 5      fragments = [
 6          "me3JSrEcT+rKpxcEWXVu02FAjDr1NcXtDNqh5VwSVsf47ameaHvH47zmKVBNRKEphw==",
 7          "TtoDPEj54cMniF1HO0110UmAcMOVU7Bk",
 8          "jHXaa9x2p1mrGhMrA2nJhIrFGE/Tu5p01CM9p+11rOTx",
 9          "ZbrjCSEDoajyBM45XlURJPcmuiO90FvuWX6sOagtLN7E0xqN9IpqJ5Wk=",
10          "Uvo6noeBzccc492sEb/p8hjfSc2c8TbgGnxKfPCYVRJjdxETCcF/Y0=",
11          "PUDdiclejecRkd94M8cvHp8nsLW56902im7cbZ1h7f8MLbqT",
12          "aGhoLCExORETDm8tCh0xMy5vc3t1dj9oaGg=",
13          "+lIPmi6mOreftnpyTSJHVyqVbeKHjfCwM5ZSPNTV7/0yu5IATyghKEtn4CJH9/bxGuD+AAE3NDG6fg=="
14      ]
15
16      ciphertext = b""
17      for i, frag in enumerate(fragments):
18          try:
19              missing_padding = len(frag) % 4
20              if missing_padding:
21                  frag += '=' * (4 - missing_padding)
22              ciphertext += base64.b64decode(frag)
23          except Exception as e:
24              print(f"Error saat men-decode fragmen #{i+1}: {e}")
25          return
26
27      print(f"[*] Total panjang ciphertext setelah digabung: {len(ciphertext)} bytes")
28
29      xor_key = 0x42
30
31      decrypted_data = bytearray()
32      for byte in ciphertext:
33          decrypted_data.append(byte ^ xor_key)
34
35      flag_pattern = rb"ncs\{.*?\}"
36
37      match = re.search(flag_pattern, decrypted_data)
38
39      if match:
40          found_flag = match.group(0).decode('utf-8')
41          print("\n[+] Flag berhasil ditemukan dan diekstrak!")
42          print(f"    {found_flag}")
43      else:
44          print("\n[-] Flag tidak ditemukan di dalam data hasil dekripsi.")
45          print("    Mungkin ada kesalahan pada daftar fragmen atau kunci.")
46
47  if __name__ == "__main__":
48      extract_the_flag()

```

Saat kode tersebut dijalankan, akan menghasilkan hal berikut dan menemukan flagnya:

## APTIKOM

# Nusantara Cyber Security 2025

```
PS D:\kuliah> python solve.py
[*] Total panjang ciphertext setelah digabung: 308 bytes
[*] Total panjang ciphertext setelah digabung: 308 bytes

[+] Flag berhasil ditemukan dan diekstrak!
ncs{SQL-oH_sql-1974}
```

#### 4. Soal No 4 (Peser dari Pejuang)

**Flag:**

ncs{this\_is\_a\_message}

**Deskripsi:**

Seorang pejuang kemerdekaan meninggalkan pesan rahasia yang disandikan menggunakan metode klasik. Pesan tersebut ditemukan dalam bentuk berikut:

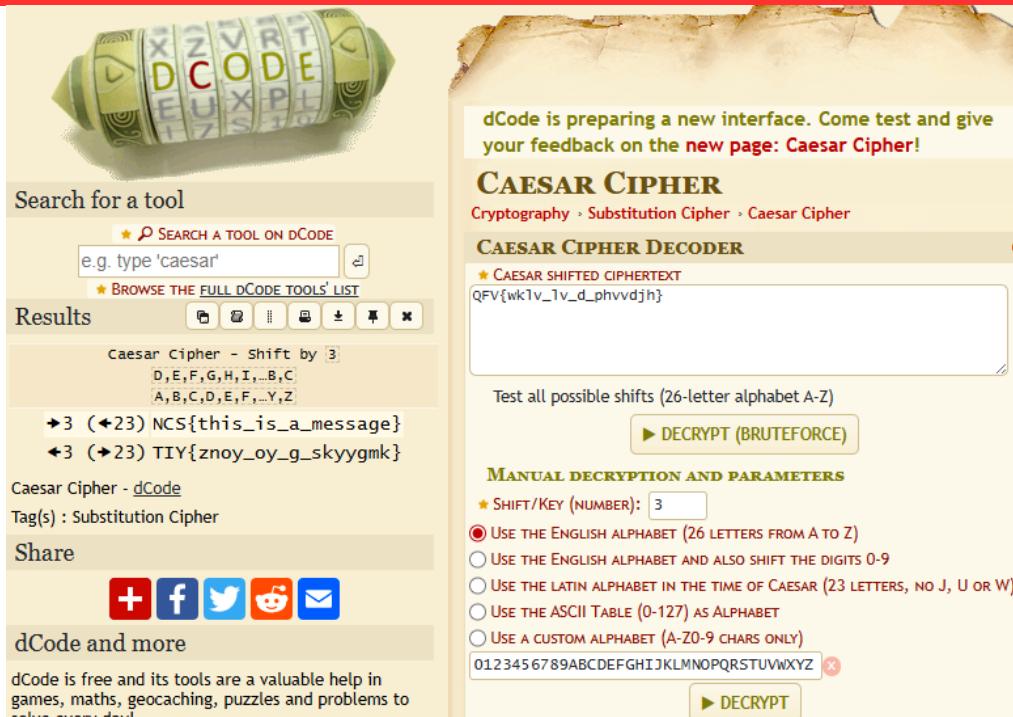
**Wklv phvvdjh lv hqfubswhg: QFV{wklv\_lv\_d\_phvvdjh}**

**Solusi:**

Metode klasik yang langsung terpikirkan di awal merupakan caesar cipher karena kami sedang menjalani mata kuliah kriptografi juga di kampus, dengan format yang disampaikan adalah ncs{}, maka menyelesaikan bagian QFV terlebih dahulu dan mendapatkan bahwa kuncinya adalah pergeseran 3 huruf dan langsung melakukan decode hingga menemukan NCS{this\_is\_a\_message} (yang ternyata ncs dan bukan NCS).

# APTIKOM

## Nusantara Cyber Security 2025



The screenshot shows the dCode Caesar Cipher Decoder interface. At the top, it says "dCode is preparing a new interface. Come test and give your feedback on the new page: Caesar Cipher!". Below that, the title "CAESAR CIPHER" and subtitle "Cryptography > Substitution Cipher > Caesar Cipher" are displayed. The main section is titled "CAESAR CIPHER DECODER". It shows the input text "QFV{wk1v\_1v\_d\_phvvdjh}" and a button "► DECRYPT (BRUTEFORCE)". Below the input, there's a note: "Test all possible shifts (26-letter alphabet A-Z)" and a "► DECRYPT" button. On the left, under "Results", it shows the decrypted message "this\_is\_a\_message" with a shift of 3. Other sections include "Caesar Cipher - Shift by 3" and "Caesar Cipher - dCode". There are also sections for "Share" with social media icons and "dCode and more" with a note about its usefulness.

### 5. Soal No 5 (Everything has changed)

**Flag:**

ncs{Pdf5\_C4N\_8E\_P4Rt14Lly\_rECOveREd\_1f\_they\_4rE\_D4m49Ed\_O  
r\_enCRYpTEd}

**Solusi:**

Diberikan sebuah file pdf yang rusak dan tidak bisa dibuka, kami curiga jika permasalahannya ada di file signaturenya. Menggunakan software hxd kami langsung mengecek header dari pdf tersebut. Ternyata benar saja bahwa headernya kurang untuk file signature pdf

# APTIKOM

## Nusantara Cyber Security 2025

HxD - [D:\IDM\Sukuna (1).pdf]

File Edit Search View Analysis Tools Window Help

memdump.mem Sukuna (1).pdf

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	B8 8B 05 C9 33 00 00 C7 00 01 00 00 00 48 8B 05	É3..Ç.....H.
00000010	4C 33 00 00 66 81 38 4D 5A 75 0F 48 63 50 3C 48	L3..f.8MZu.HcP<H
00000020	01 D0 81 38 50 45 00 00 74 66 48 8B 05 6F 33 00	.D.8PE..tfH. <o3.< o3=""></o3.<>
00000030	32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 29 20 2F	2 0 R/Lang(en) /
00000040	53 74 72 75 63 74 54 72 65 65 52 6F 6F 74 20 33	StructTreeRoot 3
00000050	31 20 30 20 52 2F 4D 61 72 6B 49 6E 66 6F 3C 3C	1 0 R/MarkInfo<<
00000060	2F 4D 61 72 6B 65 64 20 74 72 75 65 3E 3E 2F 4D	/Marked true>>/M
00000070	65 74 61 64 61 74 61 20 35 36 20 30 20 52 2F 56	etadata 56 0 R/V
00000080	69 65 77 65 72 50 72 65 66 65 72 65 6E 63 65 73	iewerPreferences
00000090	20 35 37 20 30 20 52 3E 3E 0D 0A 65 6E 64 6F 62	57 0 R>>.endob
000000A0	6A 0D 0A 32 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54	j..2 0 obj..<</T
000000B0	79 70 65 2F 50 61 67 65 73 2F 43 6F 75 6E 74 20	ype/Pages/Count
000000C0	37 2F 4B 69 64 73 5B 20 33 20 30 20 52 20 37 20	7/Kids[ 3 0 R 7

Special editors

Data inspector

Binary (8 bit) 01001000

Int8 go to: 72

UInt8 go to: 72

Int16 go to: -29880

UInt16 go to: 35656

Byte order

Little endian    Big endian

Hexadecimal basis (for integral numbers)

Results

Checksum Search (0 hits)

Offset Excerpt (hex) Excerpt (text)

Terlihat disini bahwa pada header yang seharusnya terdapat file signature pdf malah kosong. Akhirnya kami mengcopy header dari pdf yang normal ke dalam pdf sukuna tersebut yang bermasalah

HxD - [D:\IDM\Sukuna.pdf]

File Edit Search View Analysis Tools Window Help

memdump.mem Sukuna (1).pdf Sukuna.pdf

Offset(h)	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Decoded text
00000000	B5 50 44 46 2D 31 2E 35 0D 0A 25 B5 B5 B5 0D	PDF-1.5..%ppmu.
00000010	0A 31 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54 79 70	.1 0 obj..<</Typ
00000020	65 2F 43 61 74 61 6C 6F 67 2F 50 61 67 65 73 20	e/Catalog/Pages
00000030	32 20 30 20 52 2F 4C 61 6E 67 28 65 6E 29 20 2F	2 0 R/Lang(en) /
00000040	53 74 72 75 63 74 54 72 65 65 52 6F 6F 74 20 33	StructTreeRoot 3
00000050	31 20 30 20 52 2F 4D 61 72 6B 49 6E 66 6F 3C 3C	1 0 R/MarkInfo<<
00000060	2F 4D 61 72 6B 65 64 20 74 72 75 65 3E 3E 2F 4D	/Marked true>>/M
00000070	65 74 61 64 61 74 61 20 35 36 20 30 20 52 2F 56	etadata 56 0 R/V
00000080	69 65 77 65 72 50 72 65 66 65 72 65 6E 63 65 73	iewerPreferences
00000090	20 35 37 20 30 20 52 3E 3E 0D 0A 65 6E 64 6F 62	57 0 R>>.endob
000000A0	6A 0D 0A 32 20 30 20 6F 62 6A 0D 0A 3C 3C 2F 54	j..2 0 obj..<</T
000000B0	79 70 65 2F 50 61 67 65 73 2F 43 6F 75 6E 74 20	ype/Pages/Count
000000C0	37 2F 4B 69 64 73 5B 20 33 20 30 20 52 20 37 20	7/Kids[ 3 0 R 7

Special editors

Data inspector

Binary (8 bit) 00100101

Int8 go to: 37

UInt8 go to: 37

Int16 go to: 20517

UInt16 go to: 20517

Byte order

Little endian    Big endian

Hexadecimal basis (for integral numbers)

Results

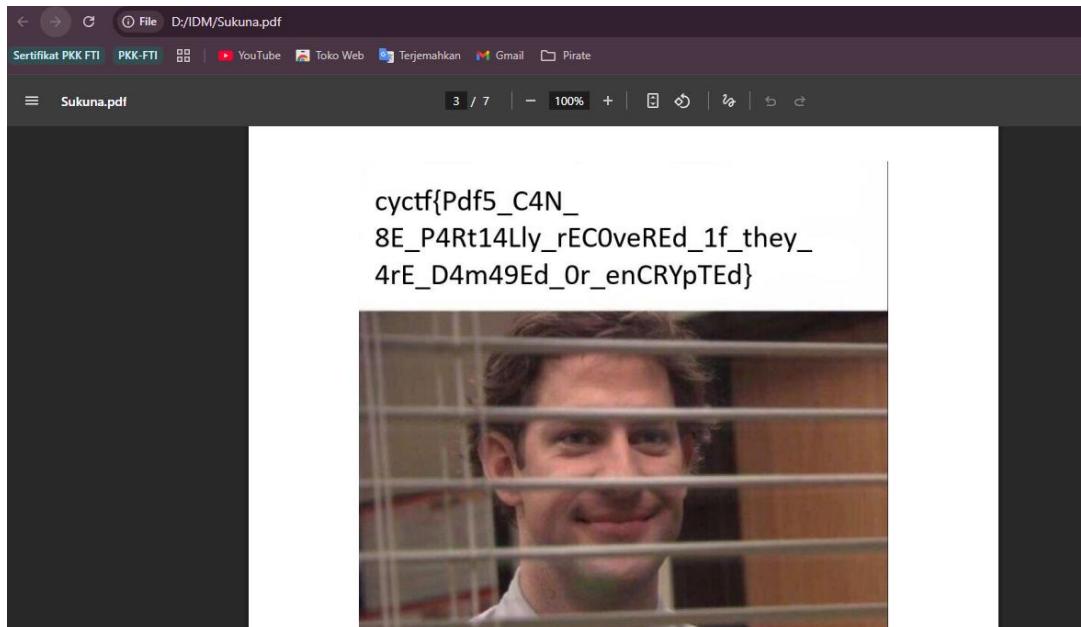
Checksum Search (0 hits)

Offset Excerpt (hex) Excerpt (text)

# **APTIKOM**

## **Nusantara Cyber Security 2025**

Setelah kami tambahkan akhirnya file pdf bisa terbuka dan menampilkan 7 halaman, dan flag ditemukan pada halaman 3



Flag butuh disesuaikan sehingga hasilnya  
ncs{Pdf5\_C4N\_8E\_P4Rt14Lly\_rEC0veREd\_1f\_they\_4rE\_D4m49Ed\_Or\_enCRYpTEd}