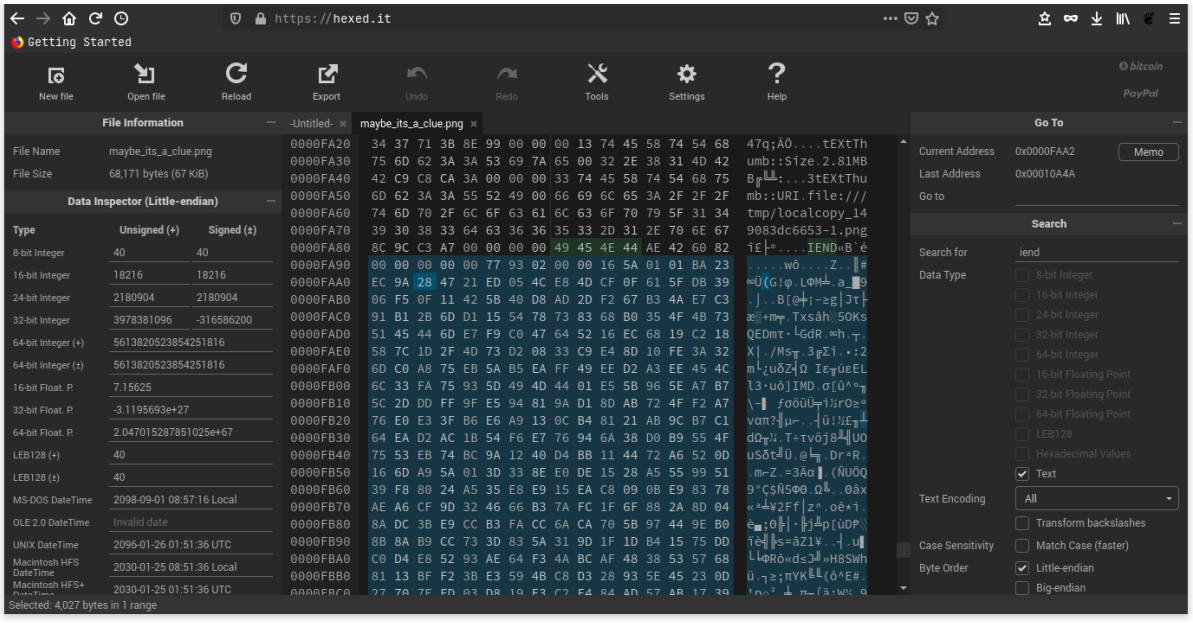
Proof of Work “Basic Steg”

Diberikan file MrSteg.zip, di dalamnya terdapat file maybe_its_a_clue.png. Dianalisa dan terdapat Atom zip yang di reverse setiap bytenya

```
000108E0   75 6D 2E A5   BA CC FF D4   38 C9 CB 86   6A 0E CB F7   um......8...j...
000108F0   F9 B6 28 EF   20 4A DD 81   9E FD F6 9E   F0 6D F6 16   ..(. J.......m..
00010900   C7 1C 8C 3A   A3 B7 12 BF   ED 90 7B AA   3B AB 90 70   ...:......{.;..p
00010910   6C AD DD 99   07 E6 87 C6   4A F0 7F C7   23 25 15 65   l.......J...#%.e
00010920   F8 51 81 B0   AB 9F E7 53   FE 8F 77 FF   FA 64 B0 44   .Q.....S..w..d.D
00010930   B5 CD 28 1A   03 FA 0F C3   F7 B9 E4 CC   5F C4 88 4C   ..(........._..L
00010940   45 B1 A9 02   F7 12 3F E5   9B F9 6C E1   8C 7D B8 9D   E.....?...l..}..
00010950   6F 3F 1A D9   40 BF 25 77   45 F6 D8 04   DD 78 3A F4   o?..@.%wE....x:.
00010960   91 F8 11 83   6D A1 1E 30   FC 4F DD D6   4F 06 68 C5   ....m..0.O..O.h.
00010970   86 38 B4 B1   E4 FF 72 9F   26 C6 A7 35   B0 BC 22 CC   .8....r.&..5..".
00010980   D2 2E 86 CD   3A EC 77 5A   99 2C 5B EA   60 44 32 E2   ....:.wZ.,[.`D2.
00010990   D0 B6 0F CF   97 19 F5 C9   B6 AD 98 47   E0 EF D6 14   ...........G....
000109A0   38 D6 D8 15   60 5B 46 2A   FB CD E8 35   69 D7 00 F3   8...`[F*...5i...
000109B0   F6 8C 5E B9   5B BF 3D B7   71 67 DE 90   1E 47 EE CF   ..^.[.=.qg...G..
000109C0   59 A0 53 ED   DC 78 88 C2   15 60 46 DF   5E 90 E2 78   Y.S..x...`F.^..x
000109D0   72 A1 11 BC   8F DE 4A 97   42 EC F5 D2   55 6F 87 9B   r.....J.B...Uo..
000109E0   23 0F 85 31   9B 69 D1 A4   E7 AB 33 BB   47 56 2A A1   #..1.i....3.GV*.
000109F0   70 56 31 DC   02 E4 87 D3   5C 42 0F 6B   30 67 E0 90   pV1.....\B.k0g..
00010A00   67 09 32 6F   E6 07 9F 4C   57 00 00 0F   6B 02 EE D0   g.2o...LW...k...
00010A10   BC 49 86 07   45 01 B4 24   5F 61 2A 18   42 00 78 63   .I..E..$_a*.B.xc
00010A20   6F 64 2E 67   67 67 67 67   61 6C 66 2B   DA 01 81 0F   od.ggggalf+....
00010A30   00 05 3B 05   09 0F 1F 61   68 70 6C 61   20 39 30 2E   ..;....ahpla 90.
00010A40   30 20 70 69   5A 6D 6F 74   41 01 AE                    0 piZmotA..
---  maybe_its_a_clue.png       --0x10A40/0x10A4B-----------------------------
```

Maka ambil file atomzip tersebut



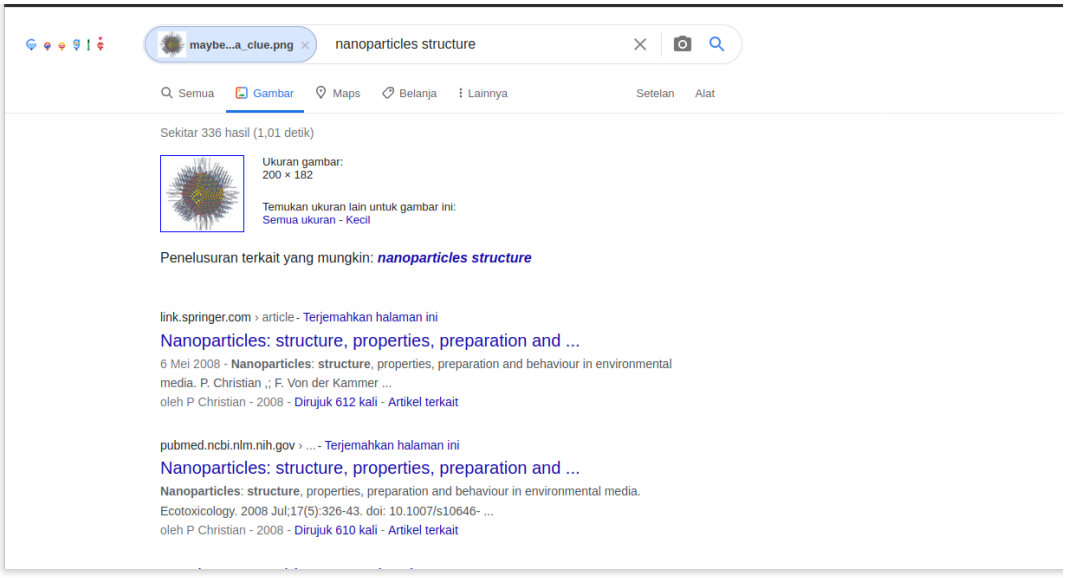
Lalu reverse setiap bytenya dengan python 3 :

```
import binascii

with open('real.nz','rb') as f :
    hexdata = f.read().hex()

hexrev = [hexdata[i:i+2] for i in range(0,len(hexdata),2)]

hexfinalrev = hexrev[::-1]

with open('rev.nz','wb') as ff:
    ff.write(binascii.unhexlify("".join(hexfinalrev)))
```

lalu hasilnya :

```
00000000   AE 01 41 74  6F 6D 5A 69  70 20 30 2E  30 39 20 61  ..AtomZip 0.09 a
00000010   6C 70 68 61  1F 0F 09 05  3B 05 00 0F  81 01 DA 2B  lpha....;......+
00000020   66 6C 61 67  67 67 67 67  2E 64 6F 63  78 00 42 18  flaggggg.docx.B.
00000030   2A 61 5F 24  B4 01 45 07  86 49 BC D0  EE 02 6B 0F  *a_$..E..I....k.
00000040   00 00 57 4C  9F 07 E6 6F  32 09 67 90  E0 67 30 6B  ..WL...o2.g..g0k
00000050   0F 42 5C D3  87 E4 02 DC  31 56 70 A1  2A 56 47 BB  .B\.....1Vp.*VG.
00000060   33 AB E7 A4  D1 69 9B 31  85 0F 23 9B  87 6F 55 D2  3....i.1..#..oU.
00000070   F5 EC 42 97  4A DE 8F BC  11 A1 72 78  E2 90 5E DF  ..B.J.....rx..^.
00000080   46 60 15 C2  88 78 DC ED  53 A0 59 CF  EE 47 1E 90  F`...x..S.Y..G..
00000090   DE 67 71 B7  3D BF 5B B9  5E 8C F6 F3  00 D7 69 35  .gq.=.[.^.....i5
000000A0   E8 CD FB 2A  46 5B 60 15  D8 D6 38 14  D6 EF E0 47  ...*F[`...8....G
000000B0   98 AD B6 C9  F5 19 97 CF  0F B6 D0 E2  32 44 60 EA  ............2D`.
000000C0   5B 2C 99 5A  77 EC 3A CD  86 2E D2 CC  22 BC B0 35  [,.Zw.:.....".."5
000000D0   A7 C6 26 9F  72 FF E4 B1  B4 38 86 C5  68 06 4F D6  ..&.r....8..h.O.
000000E0   DD 4F FC 30  1E A1 6D 83  11 F8 91 F4  3A 78 DD 04  .O.0..m.....:x..
000000F0   D8 F6 45 77  25 BF 40 D9  1A 3F 6F 9D  B8 7D 8C E1  ..Ew%.@..?o..}..
00000100   6C F9 9B E5  3F 12 F7 02  A9 B1 45 4C  88 C4 5F CC  l...?.....EL.._.
00000110   E4 B9 F7 C3  0F FA 03 1A  28 CD B5 44  B0 64 FA FF  ........(..D.d..
00000120   77 8F FE 53  E7 9F AB B0  81 51 F8 65  15 25 23 C7  w..S.....Q.e.%#.
00000130   7F F0 4A C6  87 E6 07 99  DD AD 6C 70  90 AB 3B AA  ..J.......lp..;.
00000140   7B 90 ED BF  12 B7 A3 3A  8C 1C C7 16  F6 6D F0 9E  {......:.....m..
00000150   F6 FD 9E 81  DD 4A 20 EF  28 B6 F9 F7  CB 0E 6A 86  .....J .(.....j.
00000160   CB C9 38 D4  FF CC BA A5  2E 6D 75 3D  58 70 15 65  ..8......mu=Xp.e
---  fixed       --0x0/0xFBB-----------------------------------------------------
```

Lalu analisa gambar maybe_its_a_clue.png di google images, hasilnya :



Dengan asumsi peserta sudah mencari atomzip dan tidak ketemu, maka dikorelasikan antara atom dan nano ,sehingga AtomZip diganti dengan NanoZip dan mendownload **Nanozip** di http://nanozip.ijat.my/ . Ubah pula format ekstensi menjadi **.nz** .

Setelah itu ekstrak dengan
$ nz x nanozip.nz

Hasilnya :

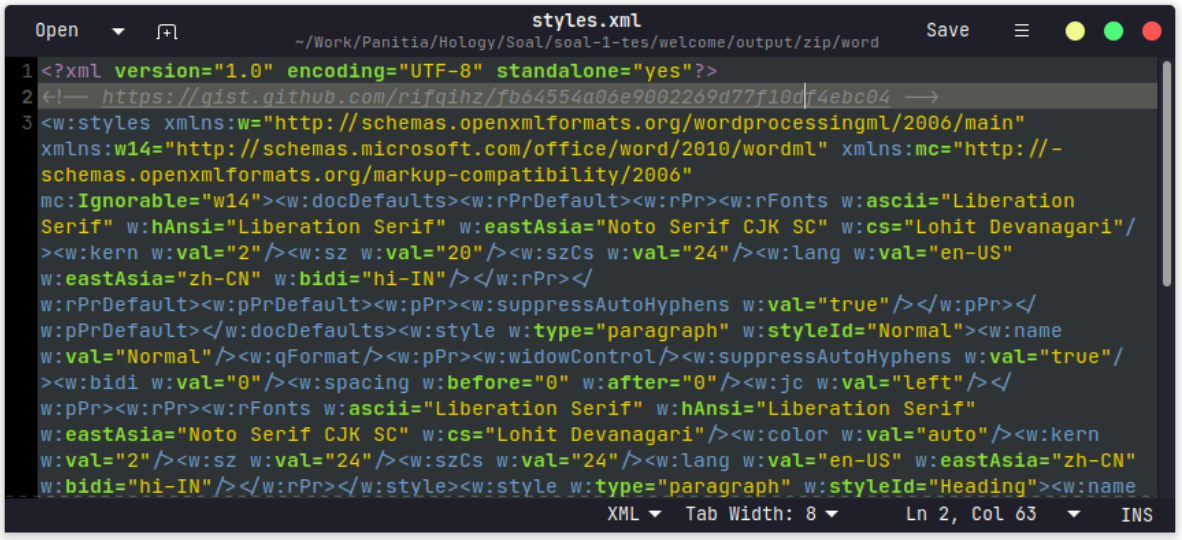
```
NanoZip 0.09 alpha/Linux64  (C) 2008-2011 Sami Runsas  www.nanozip.net
Intel(R) Core(TM) i3-7020U CPU @ 2.30GHz|2354 MHz|#2+HT|849/7841 MB
Archive: nanozip.nz
Threads: 2
Compressor #0: nz_optimum1 [13 MB]
Decompressed 5 722 bytes in 0.01s, 399 KB/s.
IO-in: 0.00s, 3934 KB/s.
```

didapat file flaggggg.docx. Setelah dianalisa terdapat anjuran untuk tidak di save dan terdapat clue “MRUWOIDEMVSXAZLS” yang didecode base32 menjadi dig deeper.

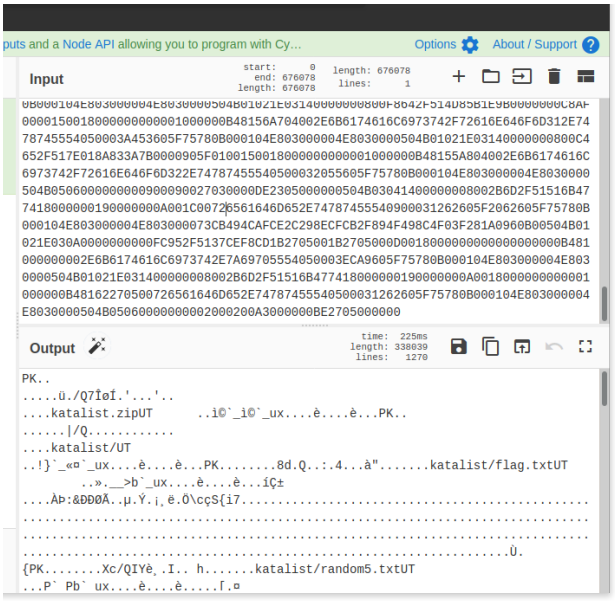
Dengan pengetahuan docx structure maka file flaggggg.docx dapat diekstrak dengan foremost / dapat diubah menjadi zip lalu diekstrak, hasilnya :

```
.
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   └── core.xml
├── _rels
│   └── .rels
└── word
    ├── document.xml
    ├── fontTable.xml
    ├── _rels
    │   └── document.xml.rels
    ├── settings.xml
    └── styles.xml

4 directories, 9 files
```

Setelah dicek terdapat link gist di dalam komen styles.xml



https://gist.github.com/rifqihz/fb64554a06e9002269d77f10df4ebc04



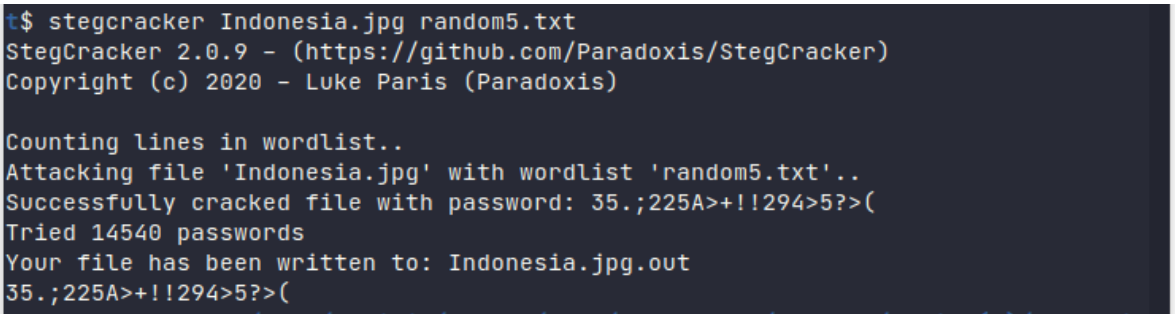
Hasilnya hex tersebut merupakan file zip . Lalu dapat mengubah hex string itu menjadi file salah satunya di https://tomeko.net/online_tools/hex_to_file.php?lang=en

Hasilnya setelah di unzip :

Lalu unzip .katalist.zip, hasilnya :

Setelah dianalisis kemungkinan besar Indonesia.jpg merupakan flagnya karena gambar nya adalah gambar bendera. Selain itu mulai dari random 1 sampai random 6 hanya random 5 yang tidak berpola. dan berdasarkan nama filenya : **katalist** yang mungkin maksudnya adalah **wordlist** maka dapat menggunakan stegcracker dengan wordlist **random5.txt** untuk melakukan crack pada Indonesia.jpg

Hasilnya :



keynya adalah “**35.;225A>+!!294>5?>(“**
(Waktu crack di laptop saya 45 detikan)

Hasilnya adalah “AXCkoAyyzmUiiwfiSQd9nznUynzik3Lo6” , jika didecode dengan base 58 hasilnya : hology3{1ts_e4sy_r1ght?}

Flag : hology3{1ts_e4sy_r1ght?}