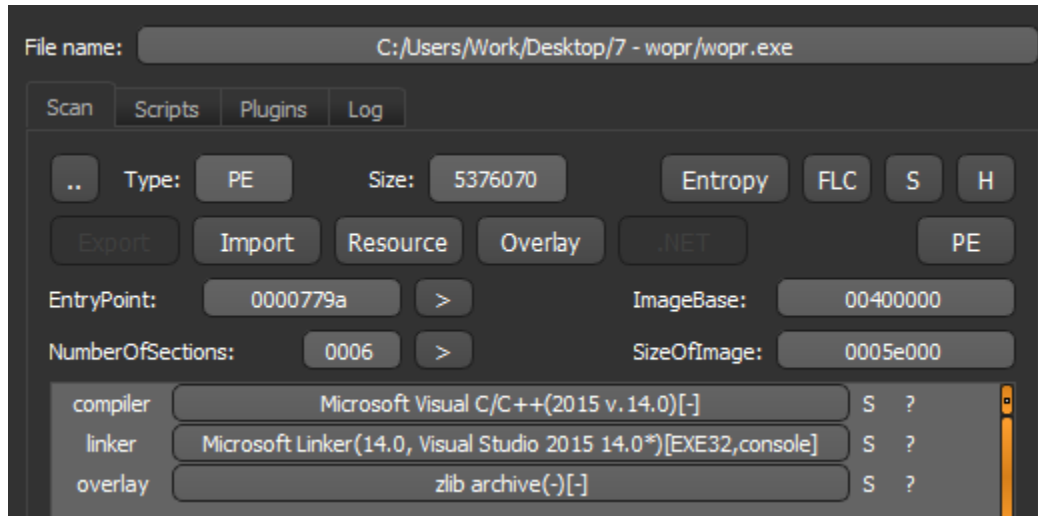


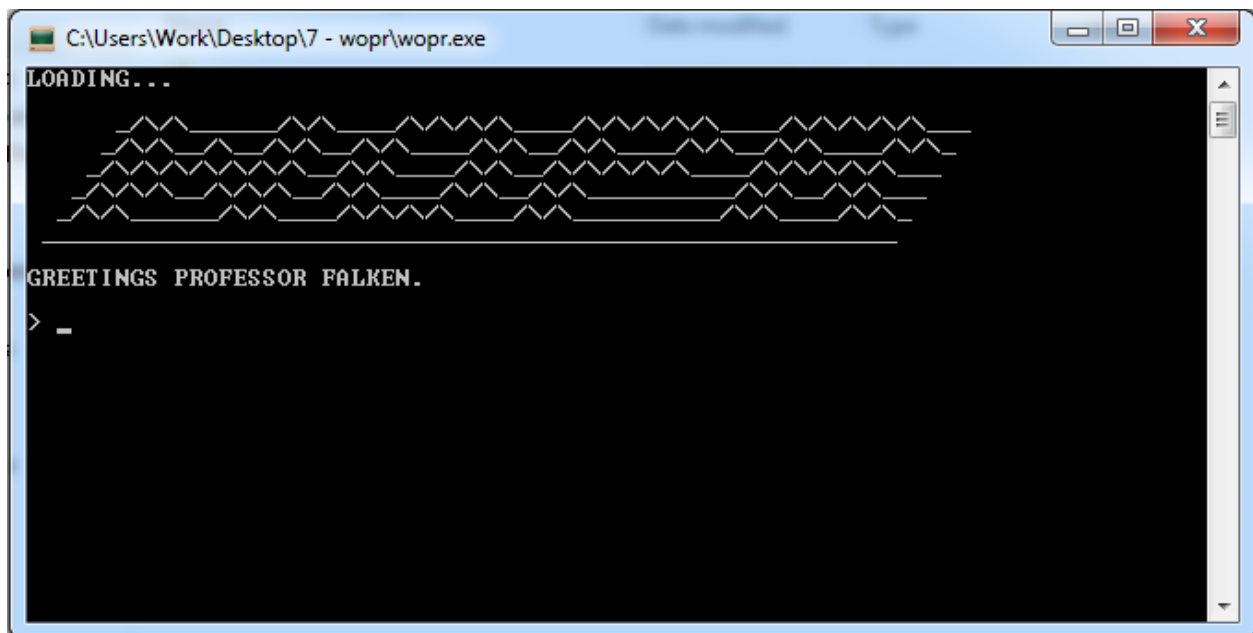
# Wopr

Kiểm tra thử chương trình ta thấy chương trình được viết bằng C/C++:



Sau khi chạy thử chương trình ta thấy:

CreateFile	C:\Users\Work\AppData\Local\Temp\_MEI4442	NAME NOT FOUND Desired Access: Read Attributes, Disposition: Op
CreateFile	C:\Users\Work\AppData\Local\Temp\_MEI4442	SUCCESS Desired Access: Read Data/List Directory, Synch
CloseFile	C:\Users\Work\AppData\Local\Temp\_MEI4442	SUCCESS
CreateFile	C:\Users\Work\AppData\Local\Temp\_MEI4442\VCRUNTIME140.dll	NAME NOT FOUND Desired Access: Read Attributes, Synchroniz
CreateFile	C:\Users\Work\AppData\Local\Temp\_MEI4442\VCRUNTIME140.dll	SUCCESS Desired Access: Generic Write, Read Attributes,
WriteFile	C:\Users\Work\AppData\Local\Temp\_MEI4442\VCRUNTIME140.dll	SUCCESS Offset: 0, Length: 69,632, Priority: Normal
WriteFile	C:\Users\Work\AppData\Local\Temp\_MEI4442\VCRUNTIME140.dll	SUCCESS Offset: 69,632, Length: 1,024, Priority: Normal
CloseFile	C:\Users\Work\AppData\Local\Temp\_MEI4442\VCRUNTIME140.dll	SUCCESS

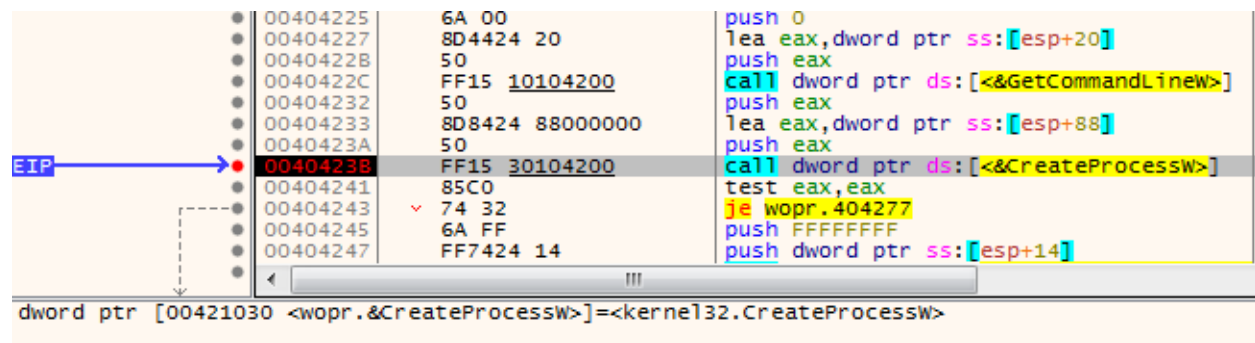


Kiểm tra folder này ta thấy

python37.dll	10/1/2019 10:45 AM	Application extens...	3,547 KB
_bz2.pyd	10/1/2019 10:45 AM	PYD File	65 KB
_ctypes.pyd	10/1/2019 10:45 AM	PYD File	99 KB
_hashlib.pyd	10/1/2019 10:45 AM	PYD File	25 KB
_lzma.pyd	10/1/2019 10:45 AM	PYD File	174 KB
_socket.pyd	10/1/2019 10:45 AM	PYD File	59 KB
_ssl.pyd	10/1/2019 10:45 AM	PYD File	95 KB

Vậy có thể chương này là một chương trình C/C++ nhúng các API python in C vào để chạy các python file trong chương trình C/C++

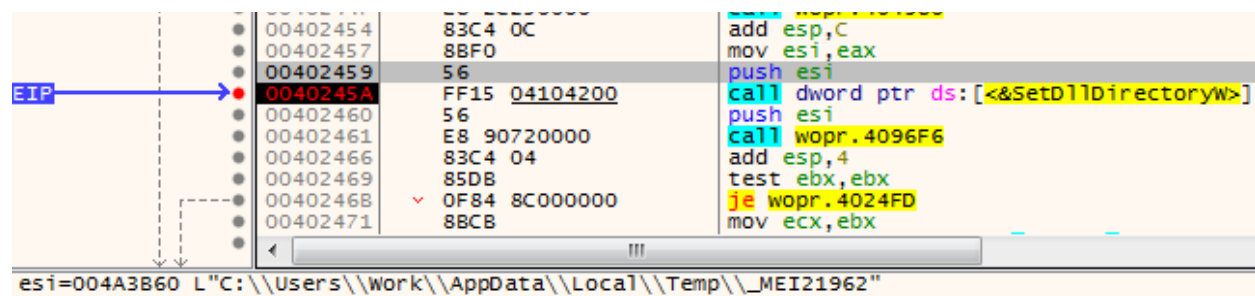
Dùng x64dbg debug chương trình ta thấy trong hàm 404120 có:



```
00404225 6A 00          push 0
00404227 8D4424 20      lea eax,dword ptr ss:[esp+20]
00404228 50            push eax
0040422C FF15 10104200 call dword ptr ds:[<&GetCommandLineW>]
00404232 50            push eax
00404233 8D8424 88000000 lea eax,dword ptr ss:[esp+88]
0040423A 50            push eax
00404238 FF15 30104200 call dword ptr ds:[<&CreateProcessW>]
00404241 85C0          test eax,eax
00404243 74 32         je wopr.404277
00404245 6A FF        push FFFFFFFF
00404247 FF7424 14     push dword ptr ss:[esp+14]
```

dword ptr [00421030 <wopr.&CreateProcessW>]=<kernel32.CreateProcessW>

Dùng plugin dbgchild để bắt được process vừa được tạo ta thấy



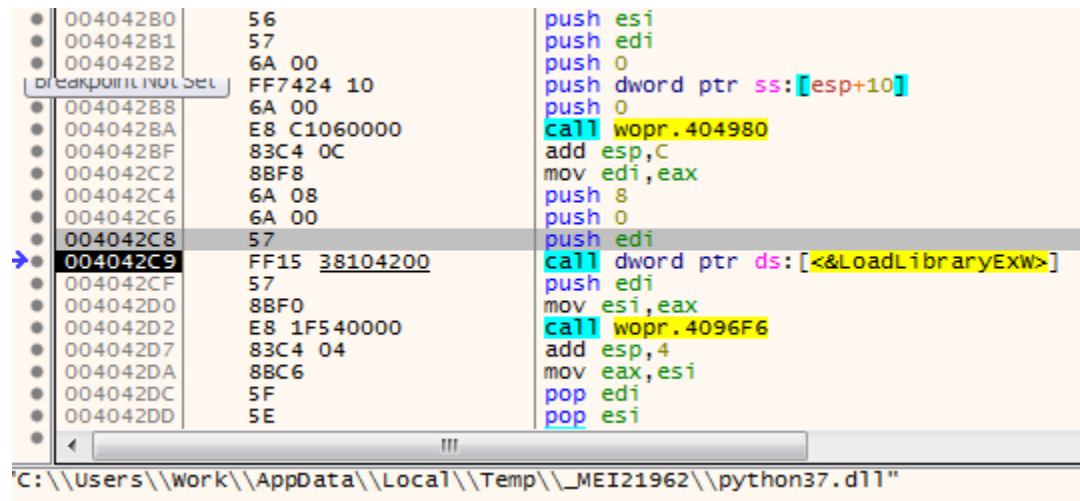
```
00402454 83C4 0C      add esp,C
00402457 8BF0        mov esi,eax
00402459 56          push esi
0040245A FF15 04104200 call dword ptr ds:[<&SetDllDirectoryW>]
00402460 56          push esi
00402461 E8 90720000 call wopr.4096F6
00402466 83C4 04      add esp,4
00402469 85DB        test ebx,ebx
0040246B 74 05         je wopr.402471
00402468 0F84 8C000000 je wopr.4024FD
00402471 8BCB        mov ecx,ebx
```

esi=004A3B60 L"C:\\Users\\work\\AppData\\Local\\Temp\\\_MEI21962"

SetDllDirectoryW vào folder chứa các dll được extract ra lúc này

Tiếp tục debug thì thấy hàm 401E50 là hàm cuối cùng x64dbg có thể chạy trước khi cửa sổ wopr hiện ra lời chào

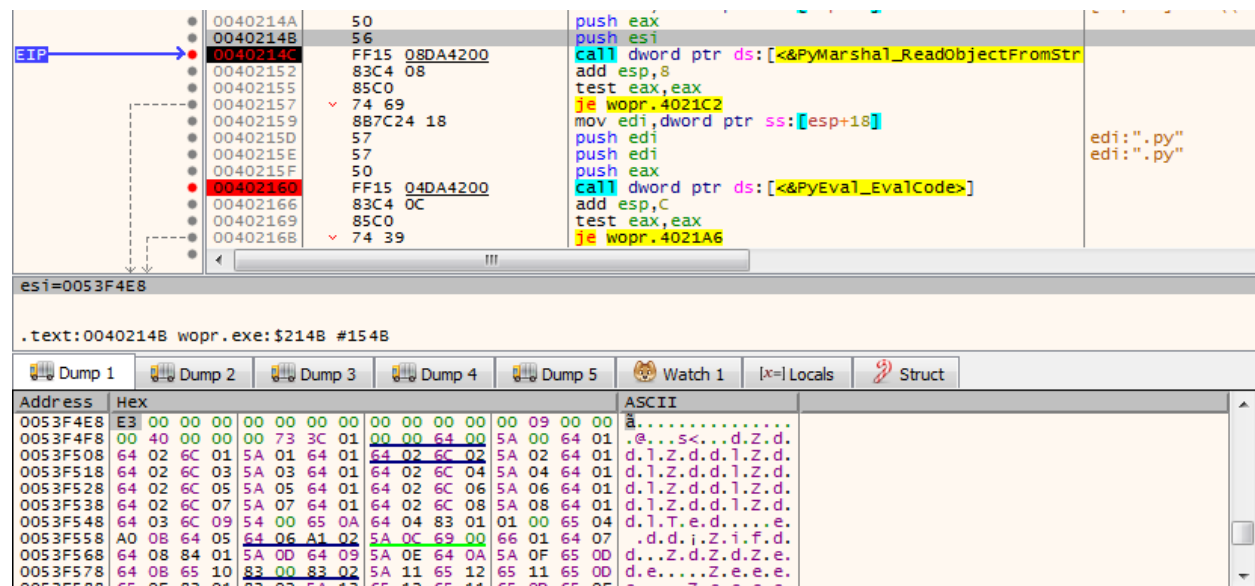
Bên trong hàm 401E50 gọi hàm 4031E0, bên trong 4042B0 có



```
004042B0 56      push esi
004042B1 57      push edi
004042B2 6A 00   push 0
004042B3 FF7424 10 push dword ptr ss:[esp+10]
004042B4 6A 00   push 0
004042B5 E8 C1060000 call wopr.404980
004042B6 83C4 0C add esp,C
004042B7 8BF8    mov edi,eax
004042B8 6A 08   push 8
004042B9 6A 00   push 0
004042BA 57      push edi
004042BB FF15 38104200 call dword ptr ds:[<&LoadLibraryExW>]
004042BC 57      push edi
004042BD 8BF0    mov esi,eax
004042BE E8 1F540000 call wopr.4096F6
004042BF 83C4 04 add esp,4
004042C0 8BC6    mov eax,esi
004042C1 5F      pop edi
004042C2 5E      pop esi
```

Vậy chương trình có sử dụng các API của python để chạy

Sau khi debug tiếp thì ta thấy



```
0040214A 50      push eax
0040214B 56      push esi
0040214C FF15 08DA4200 call dword ptr ds:[<&PyMarshal_ReadObjectFromStr>]
0040214D 83C4 08 add esp,8
0040214E 85C0    test eax,eax
0040214F 74 69   je wopr.4021C2
00402150 8B7C24 18 mov edi,dword ptr ss:[esp+18]
00402151 57      push edi
00402152 57      push edi
00402153 50      push eax
00402154 FF15 04DA4200 call dword ptr ds:[<&PyEval_EvalCode>]
00402155 83C4 0C add esp,C
00402156 85C0    test eax,eax
00402157 74 39   je wopr.4021A6
```

esi=0053F4E8

.text:0040214B wopr.exe:\$214B #154B

Address	Hex	ASCII
0053F4E8	E3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0053F4F8	00 40 00 00 00 73 3C 01 00 00 64 00 5A 00 64 01	...s<...d.Z.d.
0053F508	64 02 6C 01 5A 01 64 01 64 02 6C 02 5A 02 64 01	d.l.Z.d.d.l.Z.d.
0053F518	64 02 6C 03 5A 03 64 01 64 02 6C 04 5A 04 64 01	d.l.Z.d.d.l.Z.d.
0053F528	64 02 6C 05 5A 05 64 01 64 02 6C 06 5A 06 64 01	d.l.Z.d.d.l.Z.d.
0053F538	64 02 6C 07 5A 07 64 01 64 02 6C 08 5A 08 64 01	d.l.Z.d.d.l.Z.d.
0053F548	64 03 6C 09 5A 00 65 0A 64 04 83 01 01 00 65 04	d.l.T.e.d....e.
0053F558	A0 0B 64 05 64 06 A1 02 5A 0C 69 00 66 01 64 07	.d.d.i.Z.i.f.d.
0053F568	64 08 84 01 5A 0D 64 09 5A 0E 64 0A 5A 0F 65 00	d...Z.d.Z.d.Z.e.
0053F578	64 0B 65 10 83 00 83 02 5A 11 65 12 65 11 65 00	d.e....Z.e.e.e.
0053F588	65 05 82 01 82 02 5A 12 65 12 65 11 65 00 65 05	e...Z.e.e.e.e.

Tới đây thì thấy hàm đọc chuỗi tạo pyobject, esi chứa địa chỉ bắt đầu của pyObject và eax chứa chiều dài đọc, dump đoạn này ra ta được file pyObject, sau đó ta thêm

1 đoạn header vào đầu file này để để uncompile6.0 có thể biết được phiên bản python được sử dụng để compile ra pyObject này

42 0D 0D 0A 00 00 00 00 70 79 69 30 10 01 00 00

Ở đây chương trình có load 2 pyObject, và pyObject thứ 2 sẽ là file py chúng ta cần phân tích để tìm flag, sau khi decompile, chúng ta có file py có dạng như sau:

```
# uncompile6 version 3.4.0
# Python bytecode 3.7 (3394)
# Decompiled from: Python 2.7.16 (v2.7.16:413a49145e, Mar  4 2019, 01:30:
# Embedded file name: pyiboot02_cleanup.py
# Size of source mod 2**32: 272 bytes
"""
    Once upon a midnight dreary, while I pondered, weak and weary,
    Over many a quaint and curious volume of forgotten lore-
    While I nodded, nearly napping, suddenly there came a tapping,
    As of some one gently rapping, rapping at my chamber door-
    "'Tis some visitor," I muttered, "tapping at my chamber door-
        Only this and nothing more."

    Ah, distinctly I remember it was in the bleak December;
    And each separate dying ember wrought its ghost upon the floor
```

Tuy nhiên bạn phải check lại file này bằng HxD với đoạn string có trong dump của x64dbg vì hàm decode dùng các space và tab để làm key decode dữ liệu

```
def eye(face):
    leg = io.BytesIO()
    for arm in face.splitlines():
        arm = arm[len(arm.rstrip(' \t')):].encode()
        leg.write(arm)
```

Cuối cùng là hàm giải nén

```
for i in range(256):
    try:
        print(lzma.decompress(fire(eye(__doc__.encode()), bytes([i]) + BOUNCE)))
    except Exception:
        pass
```

Sau khi check thì thấy  $i = 74$  là giá trị đúng để giải nén ra một file py mới, lưu file này từ memory ra ổ cứng để phân tích tiếp

File py mới có đoạn đầu là

```
GREETINGS = ["HI", "HELLO", "I SUP", "AHOY", "ALOHA", "HOWDY", "GREETINGS", "ZDRAVSTVUYTE"]
STRATEGIES = ['U.S. FIRST STRIKE', 'USSR FIRST STRIKE', 'NATO / WARSAW PACT', 'FAR EAST STRATEGY', 'MIDDLE EAST WAR', 'USSR CHINA ATTACK', 'INDIA PAKISTAN WAR', 'MEDITERRANEAN WAR', 'SEATO DECAPITATING', 'CUBAN PROVOCATION', 'ATLANTIC HEAVY', 'CUBAN PARAMILITARY', 'NICARAGUAN PREEMPTIVE', 'PACIFIC TERRITORIAL', 'BURMESE THEATERWIDE', 'TURKISH DECOY', 'ARGENTINA ESCALATION', 'ICELAND MAXIMUM', 'ARABIAN THEATERWIDE', 'U.S. SUBVERSION', 'AUSTRALIAN MANEUVER', 'SUDAN SURPRISE', 'NATO TERRITORIAL', 'ZAIRE ALLIANCE', 'ICELAND', 'ENGLISH ESCALATION', 'MIDDLE EAST HEAVY', 'MEXICAN TAKEOVER', 'CHAD ALERT', 'SAUDI N', 'AFRICAN TERRITORIAL', 'ETHIOPIAN ESCALATION', 'TURKISH HEAVY', 'NATO INCURSION', 'U.S. CAMBODIAN HEAVY', 'PACT MEDIUM', 'ARCTIC MINIMAL', 'MEXICAN DOMESTIC', 'TAIWAN THEAT
```

Trong file Py mới có đoạn:

```
if b == h:
    t.typewriteln("LAUNCH CODE ACCEPTED.\n\n*** RUNNING SIMULATION ***\n")
    random.shuffle(STRATEGIES)
    for i in range(0, len(STRATEGIES), 6):
        t.write('\n'.join('{:24} {:8}'.format(k, v) for k, v in (
            [ ('STRATEGY:', 'WINNER:'), ('-' * 24, '-' * 8)] + [(_, 'NONE') for _ in
                STRATEGIES[i:i + 6]])) + '\n\n')
        time.sleep(0.5)
    t.typewriteln("**** SIMULATION COMPLETED ***\n")
    t.typewriteln('\nA STRANGE GAME.\nTHE ONLY WINNING MOVE IS\nNOT TO PLAY.\n')
    eye = [219, 232, 81, 150, 126, 54, 116, 129, 3, 61, 204, 119, 252, 122, 3, 209, 196, 15, 148, 173, 206, 246, 242,
           200, 201, 167, 2, 102, 59, 122, 81, 6, 24, 23]
    flag = fire(eye, launch_code).decode()
    t.typewrite(f"CONGRATULATIONS! YOU FOUND THE FLAG:\n\n{flag}\n")
```

Truy ngược lên trên để tìm h thì ta thấy

```
xor = [212, 162, 242, 218, 101, 109, 50, 31, 125, 112, 249, 83, 55, 187, 131, 206]
h = list(wrong())
h = [h[i] ^ xor[i] for i in range(16)]
```

Kiểm tra hàm wrong thì thấy:

```
def wrong():
    trust = windll.kernel32.GetModuleHandleW(None)

    computer = string_at(trust, 1024)
    dirty, = struct.unpack_from('=I', computer, 60)
```

Ta thấy có hàm GetModuleHandle, nếu là null thì sẽ lấy handle của process đang chạy file Py, và khi đó kết quả trả về của hàm wrong sẽ bị sai nếu như sử dụng PyCharm như mình, khi đó cần phải sửa chỗ này lại thành:

```
h_load = windll.kernel32.LoadLibraryW('C:\\Users\\Work\\Desktop\\7 - wopr\\wopr.exe')
trust = windll.kernel32.GetModuleHandleW('wopr.exe')
```

Tiếp theo b được tính toán bởi launchcode, mà b thì == h, cho nên ta phải giải hệ phương trình này để tìm được launchcode

```
# encoding map coordinates
x = list(launch_code.ljust(16, b'\0'))
b = 16 * [None]
|

# calculate missile trajectory

b[0] = x[2] ^ x[3] ^ x[4] ^ x[8] ^ x[11] ^ x[14]
b[1] = x[0] ^ x[1] ^ x[8] ^ x[11] ^ x[13] ^ x[14]
b[2] = x[0] ^ x[1] ^ x[2] ^ x[4] ^ x[5] ^ x[8] ^ x[9] ^ x[10] ^ x[13] ^ x[14] ^ x[15]
b[3] = x[5] ^ x[6] ^ x[8] ^ x[9] ^ x[10] ^ x[12] ^ x[15]
b[4] = x[1] ^ x[6] ^ x[7] ^ x[8] ^ x[12] ^ x[13] ^ x[14] ^ x[15]
b[5] = x[0] ^ x[4] ^ x[7] ^ x[8] ^ x[9] ^ x[10] ^ x[12] ^ x[13] ^ x[14] ^ x[15]
b[6] = x[1] ^ x[3] ^ x[7] ^ x[9] ^ x[10] ^ x[11] ^ x[12] ^ x[13] ^ x[15]
b[7] = x[0] ^ x[1] ^ x[2] ^ x[3] ^ x[4] ^ x[8] ^ x[10] ^ x[11] ^ x[14]
b[8] = x[1] ^ x[2] ^ x[3] ^ x[5] ^ x[9] ^ x[10] ^ x[11] ^ x[12]
b[9] = x[6] ^ x[7] ^ x[8] ^ x[10] ^ x[11] ^ x[12] ^ x[15]
b[10] = x[0] ^ x[3] ^ x[4] ^ x[7] ^ x[8] ^ x[10] ^ x[11] ^ x[12] ^ x[13] ^ x[14] ^ x[15]
b[11] = x[0] ^ x[2] ^ x[4] ^ x[6] ^ x[13]
b[12] = x[0] ^ x[3] ^ x[6] ^ x[7] ^ x[10] ^ x[12] ^ x[15]
b[13] = x[2] ^ x[3] ^ x[4] ^ x[5] ^ x[6] ^ x[7] ^ x[11] ^ x[12] ^ x[13] ^ x[14]
b[14] = x[1] ^ x[2] ^ x[3] ^ x[5] ^ x[7] ^ x[11] ^ x[13] ^ x[14] ^ x[15]
b[15] = x[1] ^ x[3] ^ x[5] ^ x[9] ^ x[10] ^ x[11] ^ x[13] ^ x[15]
```

Xor các dòng lại với nhau sao cho hệ phương trình trở thành:

```
[1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1]
```

Ta có launchcode:

```
[53, 67, 48, 71, 55, 84, 89, 50, 76, 87, 73, 50, 89, 88, 77, 66]
['5', 'C', '0', 'G', '7', 'T', 'Y', '2', 'L', 'W', 'I', '2', 'Y', 'X', 'M', 'B']
```

5C0G7TY2LWI2YXMB

Như màn hình lúc load, chương trình sẽ hỏi chúng ta input, từ file py giải nén ta thấy PLAY G là command dùng để kích hoạt game

```
elif cmd.startswith('PLAY F') or cmd == 'PLAY 1':
    t.typewriteln('GAME IS TEMPORARILY UNAVAILABLE DUE TO MAINTENANCE')
elif cmd.startswith('PLAY T') or cmd == 'PLAY 2':
    t.typewriteln('GAME IS TEMPORARILY UNAVAILABLE DUE TO MAINTENANCE')
elif cmd.startswith('PLAY G') or cmd in ('PLAY ARMAGEDDON', 'PLAY 3'):
    t.typewriteln('*** GAME ROUTINE RUNNING ***')
    break
elif cmd.startswith('PLAY '):
    t.typewriteln('THAT GAME IS NOT AVAILABLE')
```



