

# I / Phương Pháp Vẽ Trên 580VNX

*Lưu ý: Vì đã nói rất kĩ ở các File trước nên nếu có thắc mắc hãy mở ticket-support trong server Discord*

**B1.** Vào Mode 100+13an sau đó ấn phím **ON**

**B2.** Đổi Mode **Stn vào/ra(MathI/MathO)** sau đó Vào chế độ Font chữ nhỏ ([Hướng dẫn](#))

**B3.** Vào lại Mode 100+13an

**B4. Chương trình quickcopy:**

```
D820: 22 36 31 30 30 30 30 02
D828: 2E D9 48 D2 02 75 31 30
D830: C0 D9 30 30 DA 7B 31 30
D838: 30 30 18 //////////////////////////////////
D83C: 30 30 01 30 C8 03 32 30
D844: A0 9C 30 30 08 D9 30 30
D84C: A5 9C 30 30 24 D9 30 30
D854: 3E 9D 30 30 31 30 A5 9C
D85C: 30 30 30 30 30 30 36 16
D864: 32 30 30 30 80 0E 31 30
D86C: 87 D9 C2 D8 A2 D5 BC 6E
D874: 31 30 30 30 34 7B 31 30
D87C: 30 30 20 D8 32 89 06 //
D884: 30 30 74 1F 32 30 /////
```

**Giải thích ngắn gọn:** nó là ROP<sub>(phải)</sub> của từng địa chỉ<sub>(trái)</sub>

Nếu bạn không hiểu đồng trên thì cũng không cần hiểu :D.



Làm theo những gì mình nói sau đây:

**Cách bấm:** Thực hiện Basic Overflow và nhập dãy HEX dưới đây (tự tra trong bảng kí tự nhé):

Ta nhập <48 bytes> da 7b 31 30 (20 d8) c8 d1 30  
30 a2 d5 c8 e5 30 30 74 1f 32 30 30 30 33 23 (22  
36 31 30 30 30 30 02)

Thay cái đánh dấu thành các địa chỉ và ROP ở trên

*Lưu ý: nhớ xóa 3 hex thừa <01> ở giữa 2 @ sau khi xuất*

Sau đó ta bấm  

Làm tương tự các địa chỉ còn lại đến khi xong.

## B5.

<48 số bất kì> da 7b 31 30  
c2 d8 20 d8 30 30 a2 d5 50 94 30 30 30 01 74 1f  
32 30

## B6.

<48 số bất kì> da 7b 31 30  
30 30 c8 e9 30 30 a2 d5 a6 a8 30 30 c0 d9 a5 9c  
30 30 30 30 30 30 74 1f 32 30

## B7. Inject chương trình vẽ

Tương tự như trên (nhớ   khi làm xong)

00 00 30 31 30 30 01 07 D3 E3 31 18 30 DA 30 30  
30 30 30 30 30 30 7A 01 (1st line)

7E 94 30 DA 02 26 31 30 A2 D5 4E F2 31 30 DA 7B  
31 30 10 30 30 30 30 30 (2nd line)

01 30 CC 03 32 30 80 0E 31 30 30 D5 30 30 30 30  
50 99 30 30 30 30 AE 1B (3rd line)

32 30 A6 A8 30 30 0E D6 A5 9C 30 30 6C D6 30 30  
A5 9C 30 30 98 D6 30 30 (4th line)

A5 9C 30 30 30 30 30 30 02 26 31 30 90 DA 90 C7  
30 30 74 89 31 30 5E 30 (5th line)

A6 50 32 30 08 D6 8E 3B 31 30 08 40 32 30 30 30  
30 30 30 30 30 30 74 1F (6th line)

32 30 80 EB 74 89 31 30 E0 E9 02 26 31 30 76 D5  
50 94 30 30 02 00 A0 9C (7th line)

30 30 30 30 30 30 4A D0 30 30 30 30 08 40 32 30  
54 D6 30 30 30 30 30 30 (8th line)

34 7B 31 30 30 30 31 30 A6 50 32 30 78 D5 A5 9C  
30 30 30 30 30 30 74 89 (9th line)

31 30 E2 E9 32 89 B2 00 01 00 78 5C 31 30 82 D5  
36 16 32 30 76 D5 D2 90 (10th line)

30 30 74 89 31 30 30 30 02 26 31 30 30 DB 90 C7  
30 30 74 89 31 30 3C 30 (11th line)

A6 50 32 30 98 D6 8E 3B 31 30 08 40 32 30 30 30  
30 30 30 30 30 30 74 1F (12th line)



32 30 30 30 74 89 31 30 00 00 A0 9C 30 30 80 EB  
30 30 A0 9C 30 30 CC D6 (13th line)

30 30 DA 7B 31 30 30 30 31 30 78 D5 90 D5 A5 9C  
30 30 30 30 30 30 74 89 (14th line)

31 30 E2 E9 32 89 3A 00 30 30 74 1F 32 30 02 D7  
34 7B 31 30 D4 DD 00 06 (15th line)

36 9D 30 30 7E 94 30 30 DA 7B 31 30 30 30 31 30  
78 D5 90 D5 A5 9C 30 30 (16th line)

30 30 30 30 74 89 31 30 E2 E9 32 89 08 00 30 30  
74 1F 32 30 00 00 00 00 (17th line)

**Ví dụ:**

ta sẽ nhập như sau:

(0000303130300107D3E3311840DA303030303030307A0)  
DA 7B 31 30 30 30 30 30 30 30 C0 D8 74 1F 32 30`

•Lưu ý 1: Đừng nhập các dấu ngoặc đơn vô nhé vì nó chỉ là chú thích thôi.

•Lưu ý 2: Các chữ A, B, C, D, E, F là các chữ in đậm chứ ko phải biến nhớ nhé.

**B8.**

Tương tự với bước 4 nên mình sẽ chỉ để biểu thức và ảnh, còn lại các bạn tự bấm ra.

### 8.1

<48 số bất kì> da 7b 31 30  
70 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30 80

### 8.2

<48 số bất kì> da 7b 31 30  
a4 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30 ff ff

### 8.3

<48 số bất kì> da 7b 31 30  
a8 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30 ff ff

### 8.4

<48 số bất kì> da 7b 31 30  
a8 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30

### 8.5

<48 số bất kì> da 7b 31 30  
e8 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30 01

## 8.6

<48 số bất kì> da 7b 31 30  
e4 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30 30 01


## 8.7

<48 số bất kì> da 7b 31 30  
e4 da c8 d1 30 30 a2 d5 c8 e5 30 30 74 1f 32 30  
30 30 33 30

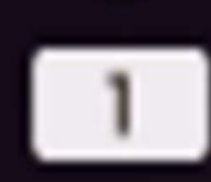
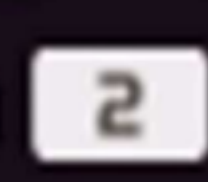
## B9:

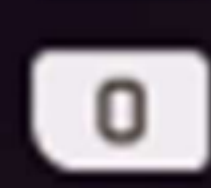
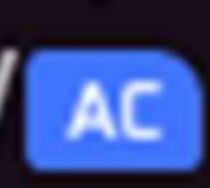
*Bước Cuối Quyết Định Bạn Thành Công Hay Không :Đ*

<48 số bất kì> da 7b 31 30 d4 dd 20 06 30 30 30  
30 36 9d 30 30 da 7b 31 30 30 30 30 01 30 30 30  
30 a6 a8 30 30 12 d1 a5 9c 30 30 30 30 30 30 da  
7b 31 30 76 d5 e0 e9 30 30 30 30 50 94 30 30 30  
30

Sau khi nhập xong bấm  . Nếu nó Clear màn hình, khả năng cao bạn đã thành công, hãy thử:

 để di chuyển

 1 đậm  2 nhạt

 0 /  để xoá

chúc may mắn

**Tiktok: @Phantatdungg**