دوره مهندسی معکوس نرم افزار

- Site: OnHexGroup.ir
- Youtube: @onhexgroup
- Telegram: onhex_ir
- Twitter: @onhexgroup
- Github: onhexgroup

نسخه ی ۳۲ و ۶۴ بیتی

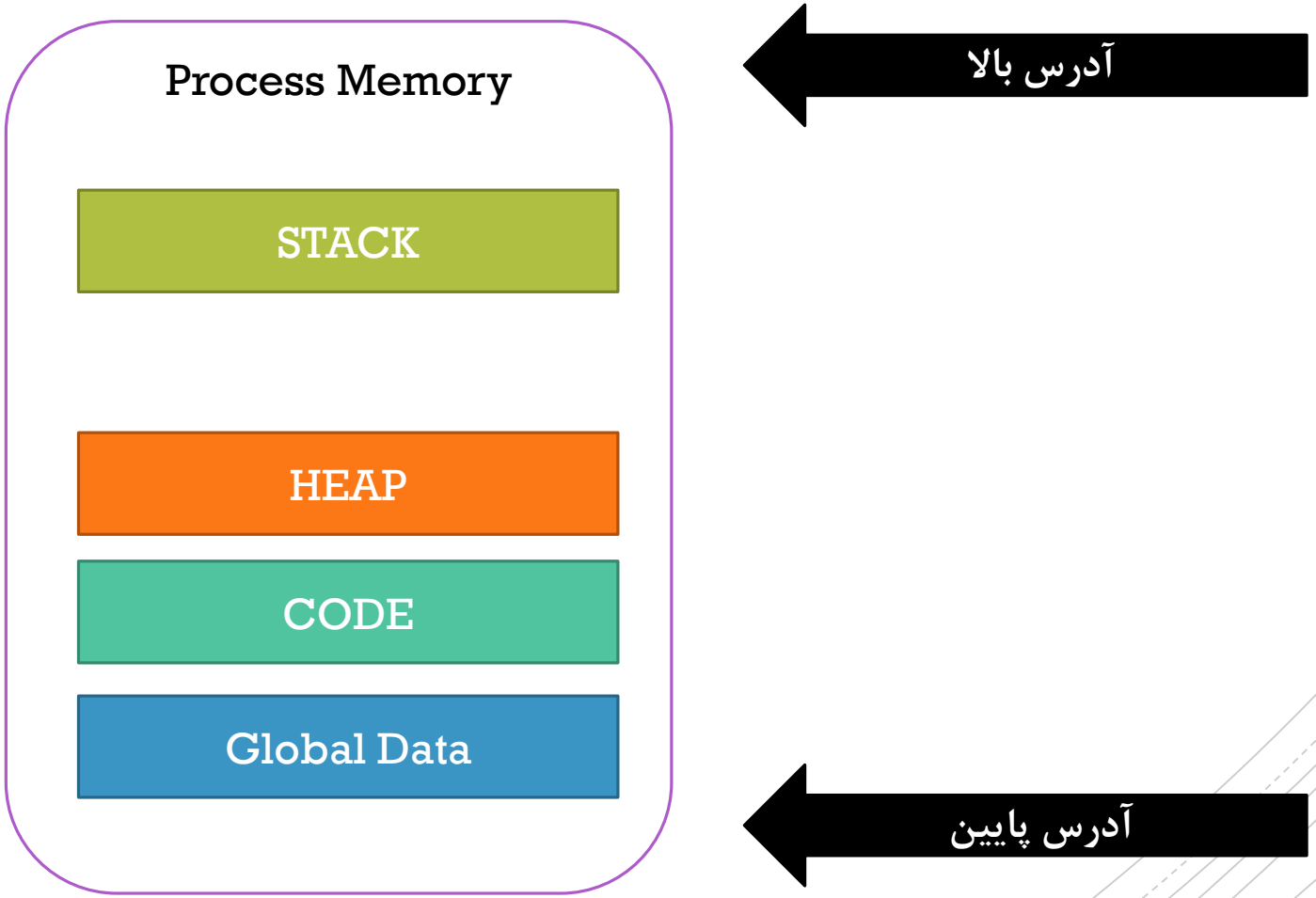
پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

- موقع اجرای برنامه در مموری ایجاد میشه.

Youtube: Onhexgroup

پشته



Onhexgroup.ir

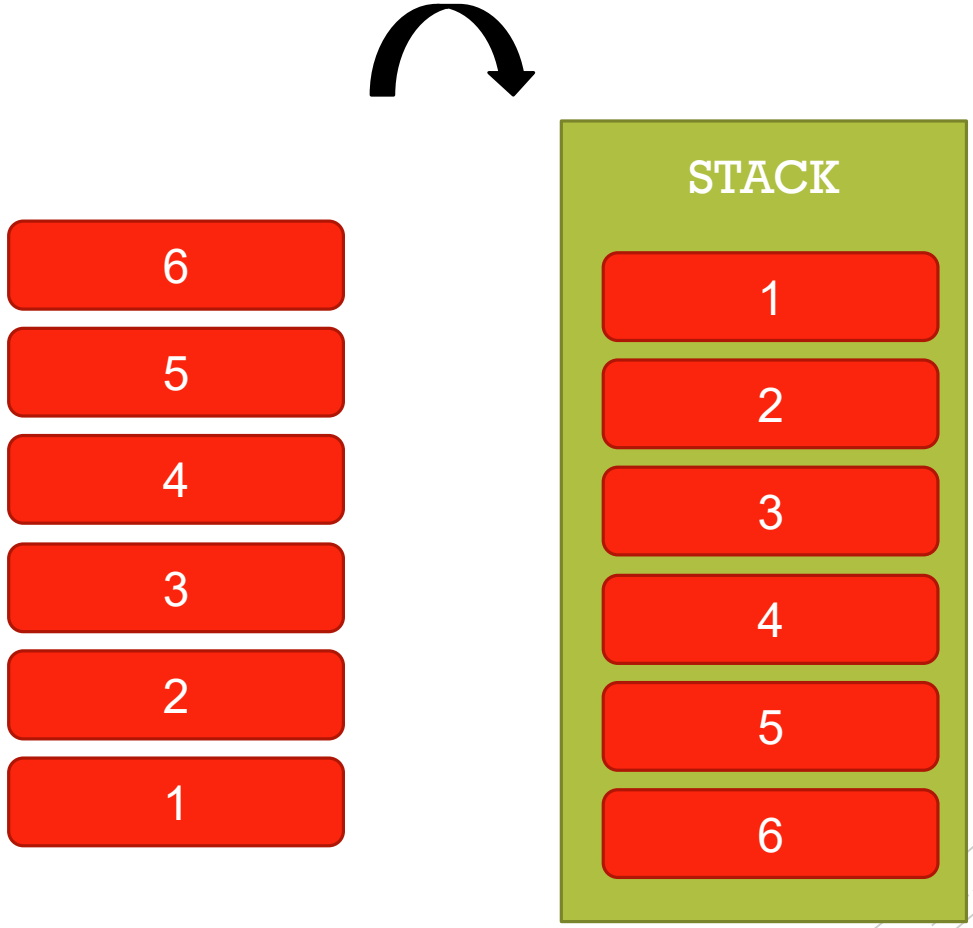
کاربردهای پشته

- آدرس بازگشت در توابع
- پارامترهای ورودی توابع
- متغیرهای محلی توابع
- وضعیت رجیسترها (فراخوانی توابع یا تغییر سطح دسترسی)

Twitter:Onhexgroup

پشته

- پشته یک ساختار داده ای براساس **LIFO** هستش.
- **LIFO = Last Input First Output**

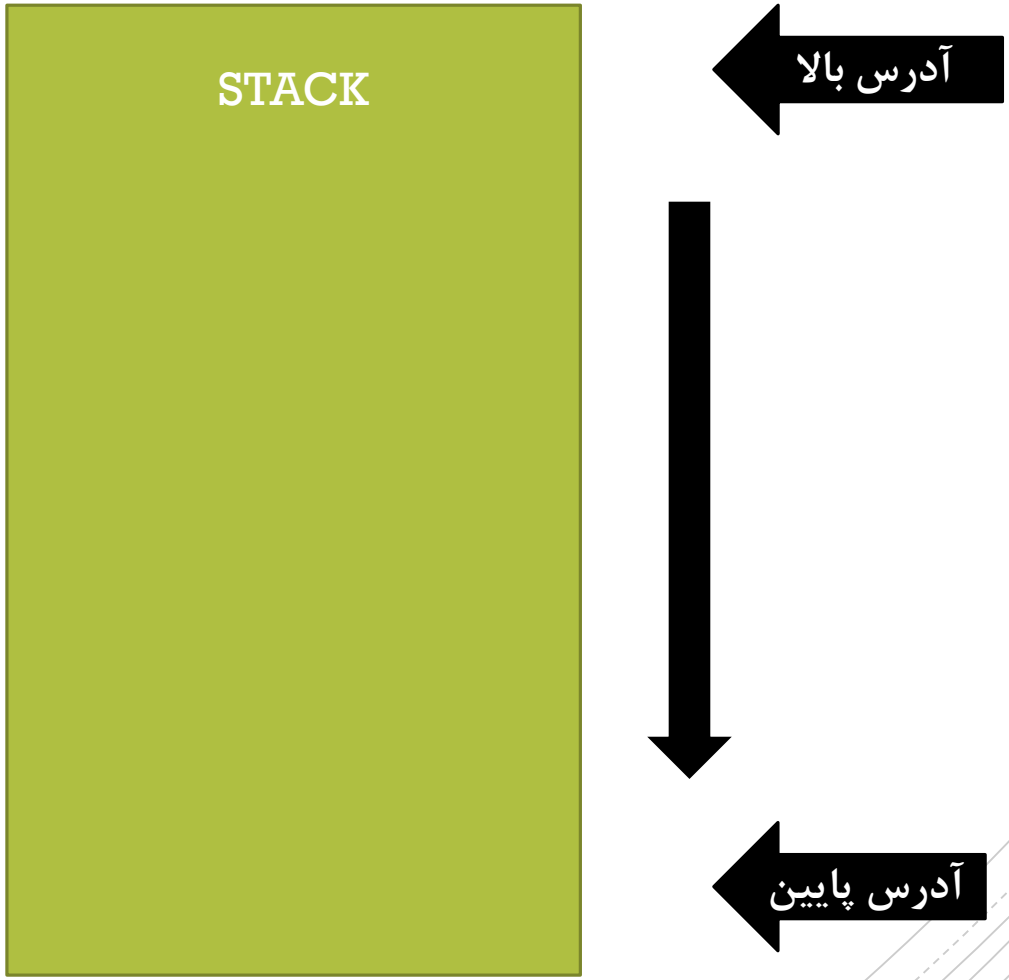


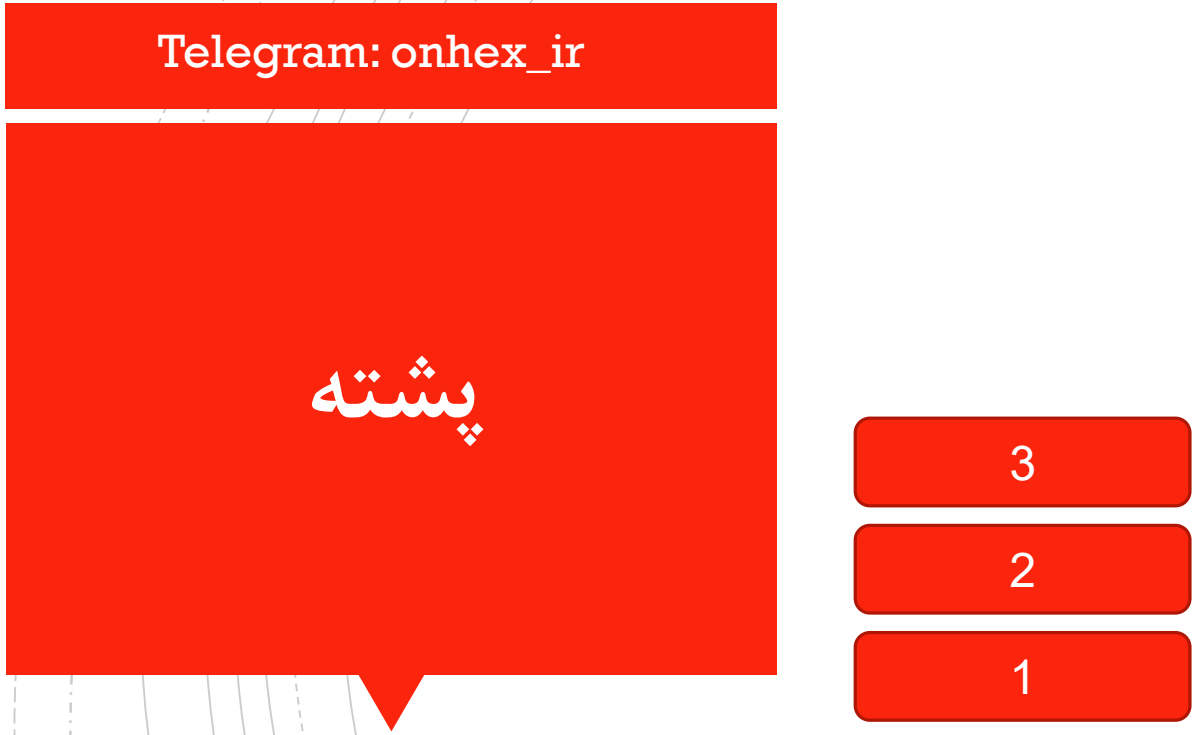
Github: Onhexgroup

پشته

- فضای آدرس دهی بصورت پیش فرض ۱ مگابایت
- هر آدرس:
  - در ۳۲ بیتی: سایز آدرس ها ۳۲ بیت یا ۴ بایت است.
  - در ۶۴ بیتی: سایز آدرس ها ۶۴ بیت یا ۸ بایت است.

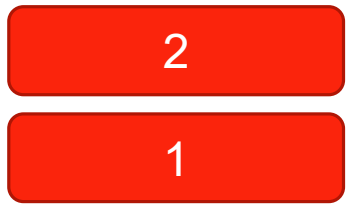
- پشته رو به آدرس های پایین تر رشد میکنه.

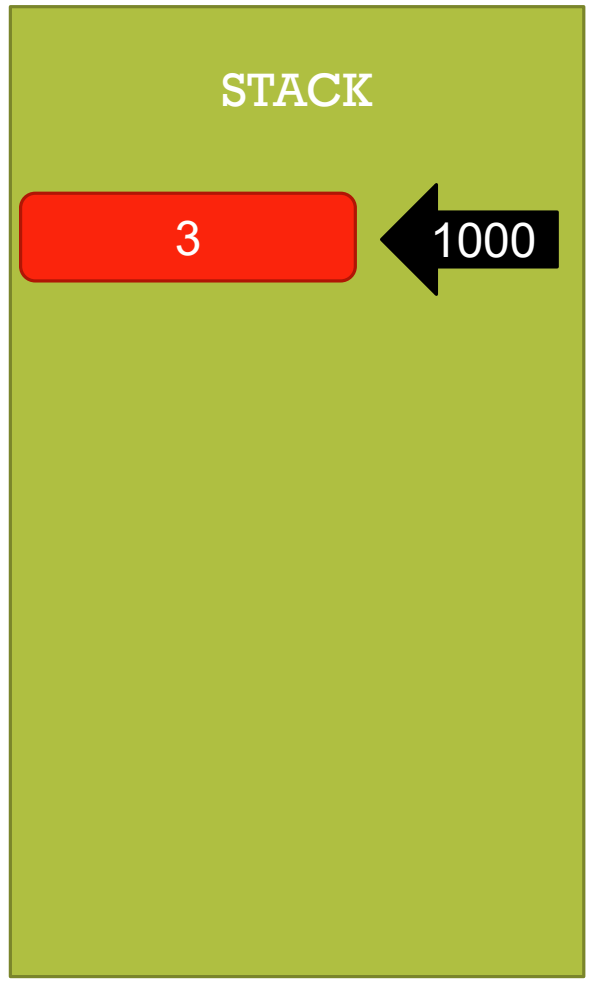




Youtube: Onhexgroup

پشته

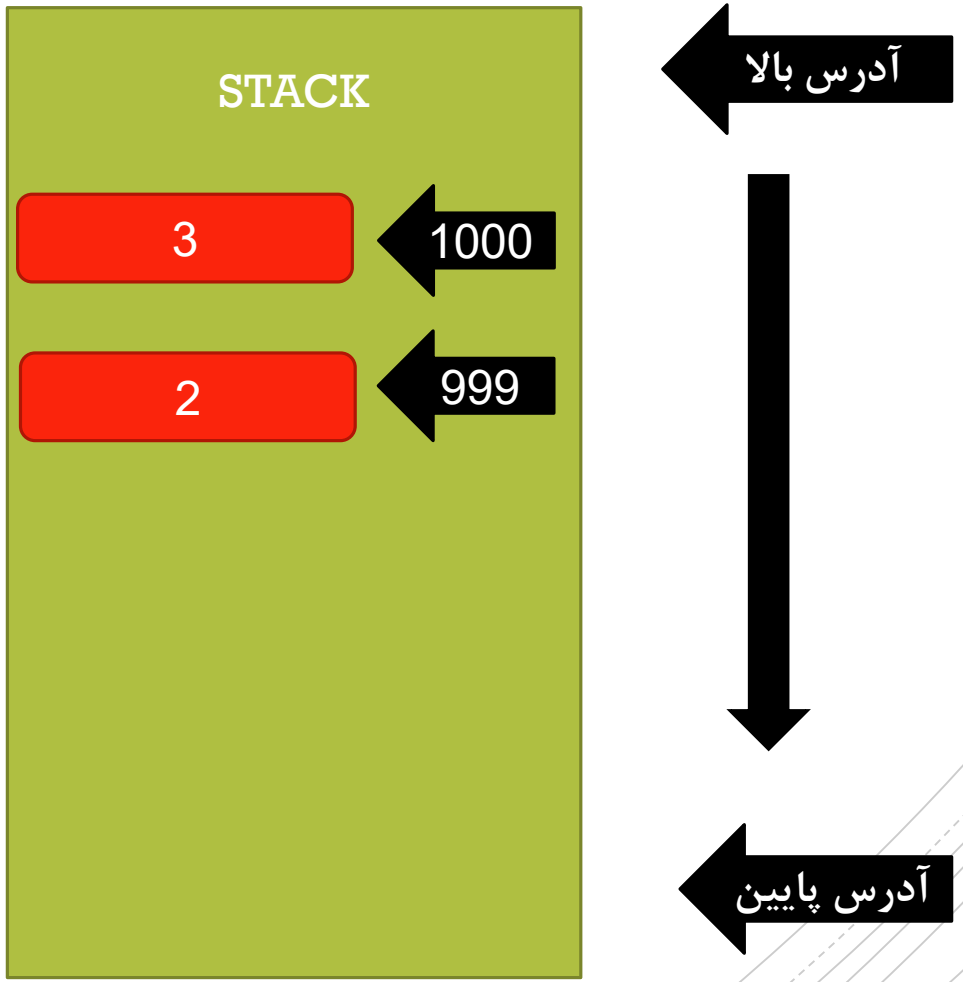




Onhexgroup.ir

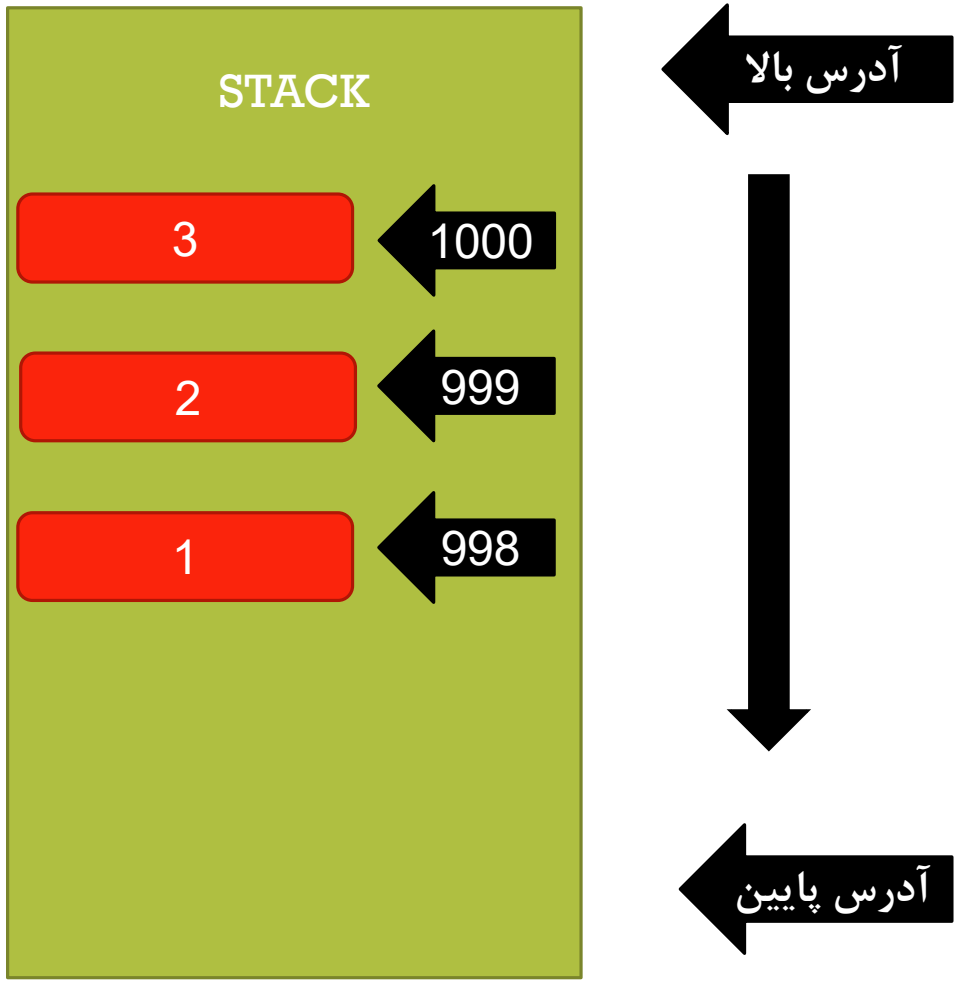
پشته

1



Github: Onhexgroup

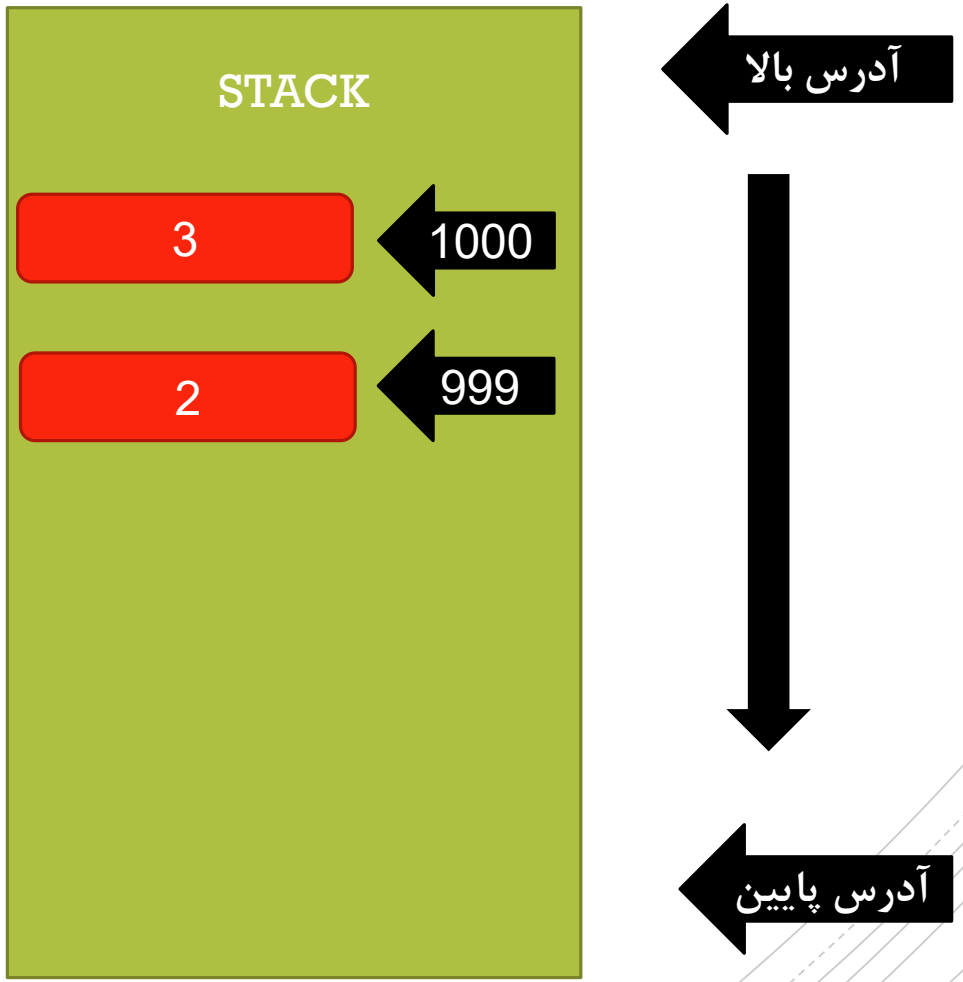
پشته



Twitter: Onhexgroup

پشته

1

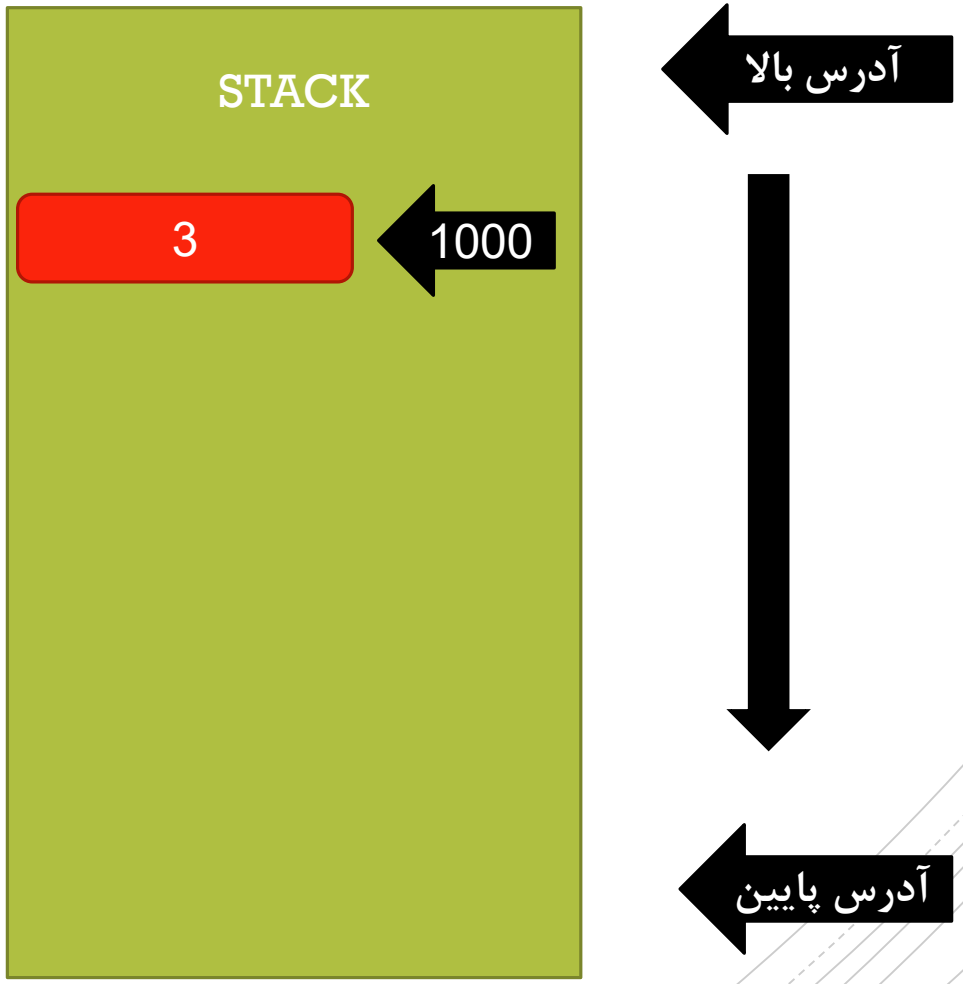


Insta: Onhexgroup

پشته

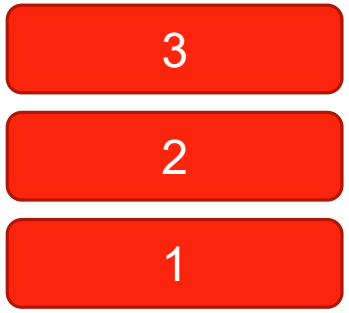
2

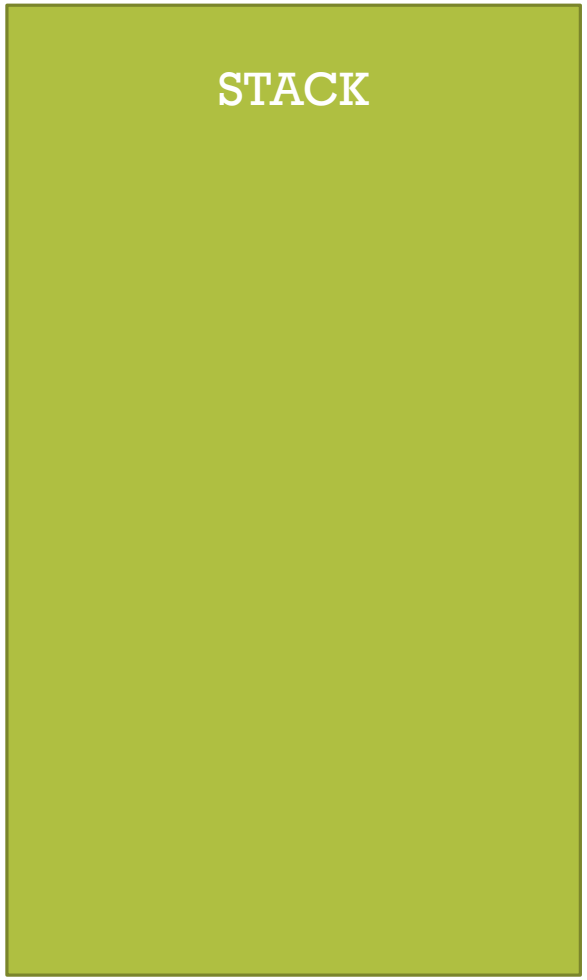
1

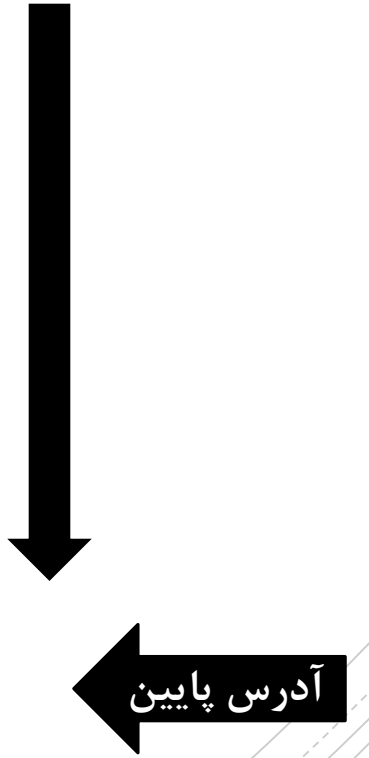


Telegram: onhex_ir

پشته







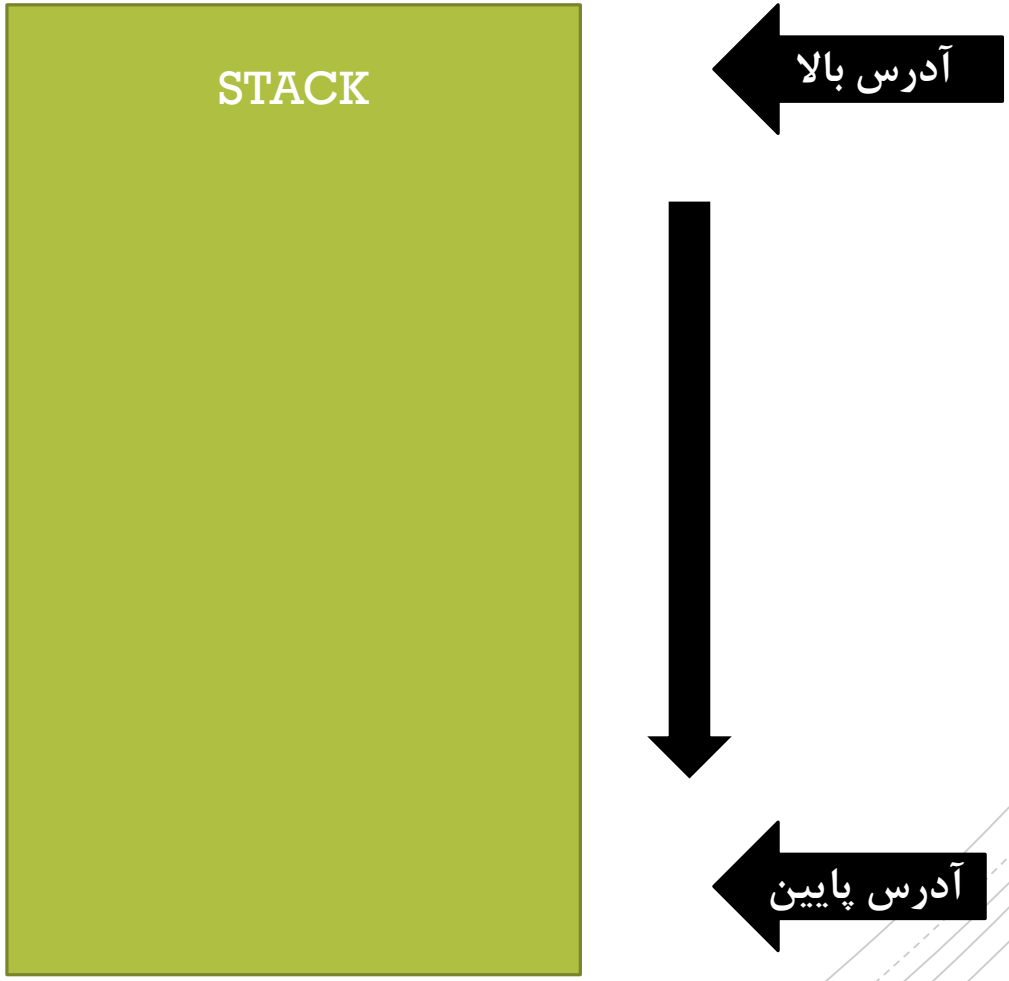
- پشته یک ساختار داده ای از نوع **LIFO**
- اشاره گر به بالای پشته: **ESP** یا **RSP**

Youtube: Onhexgroup

پشته

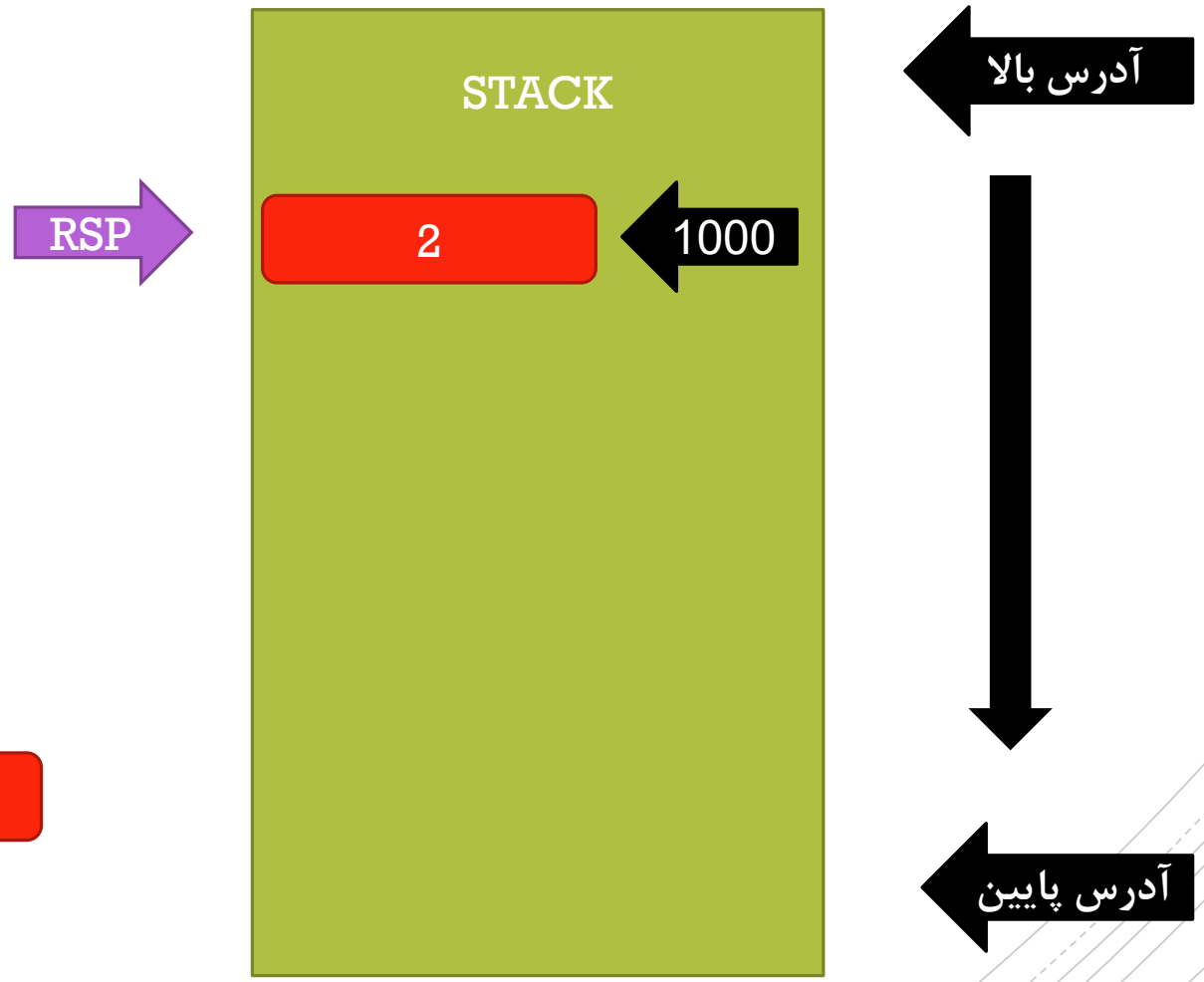
2

1



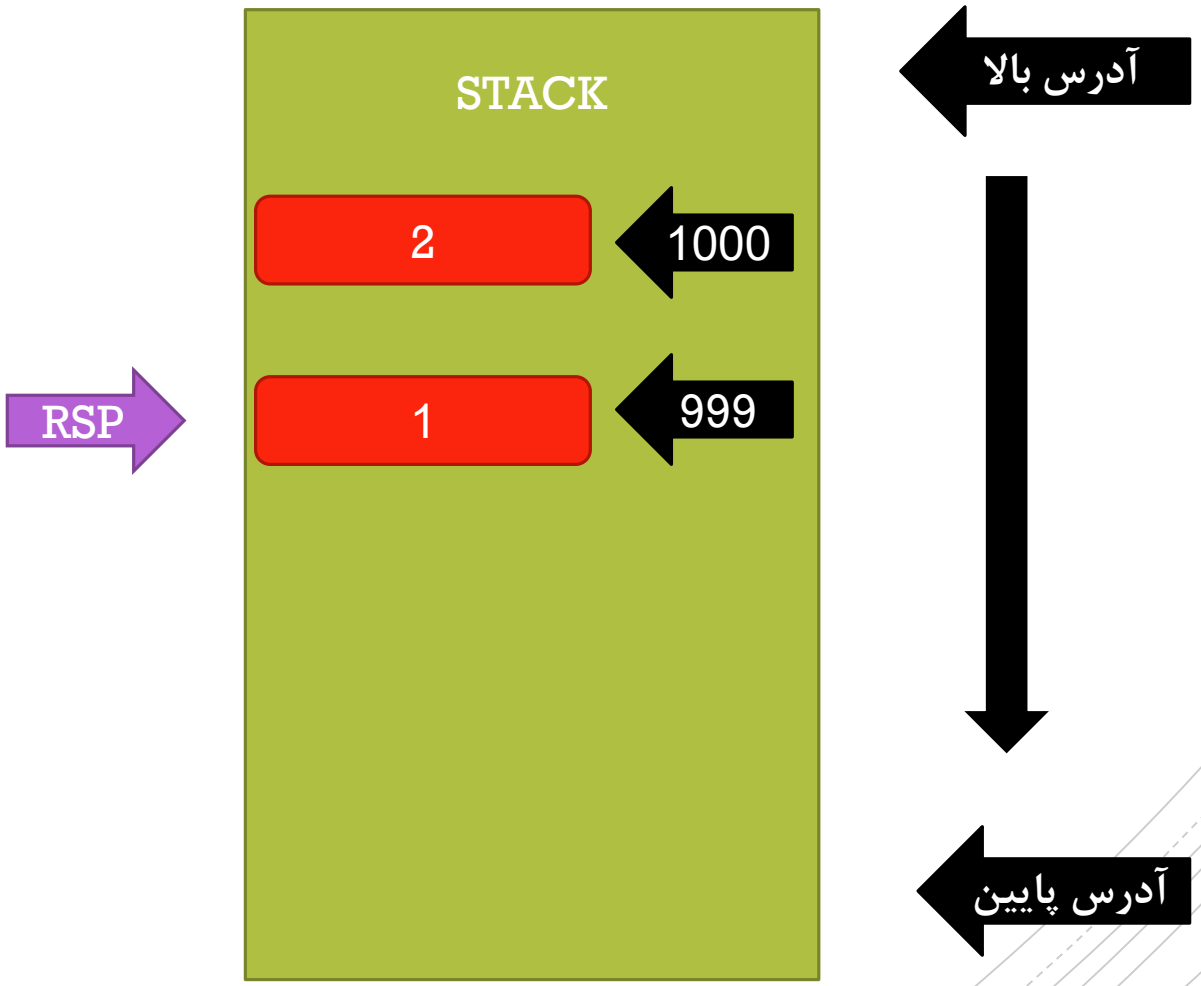
Onhexgroup.ir

پشته



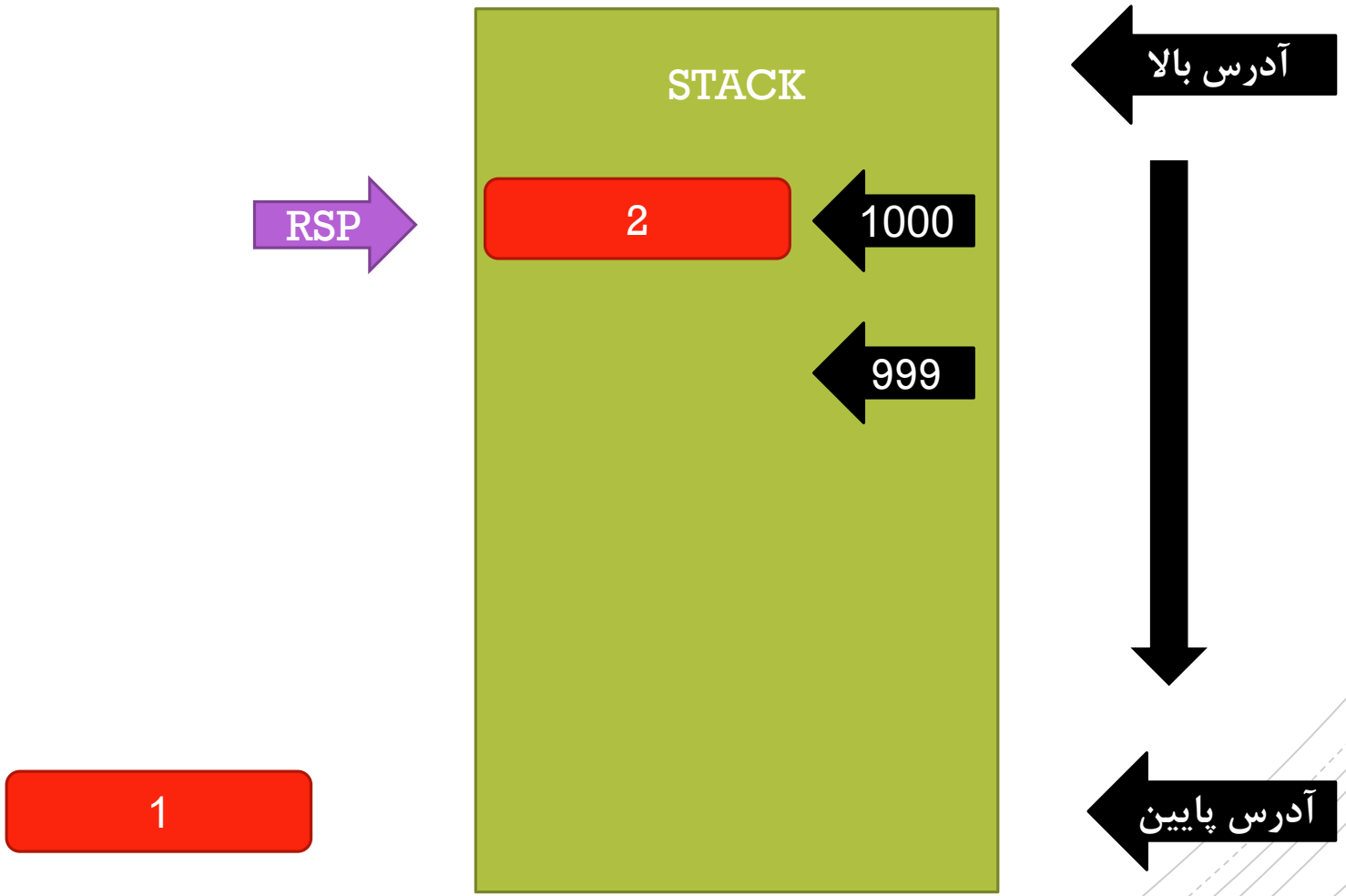
twitter: Onhexgroup

پشته



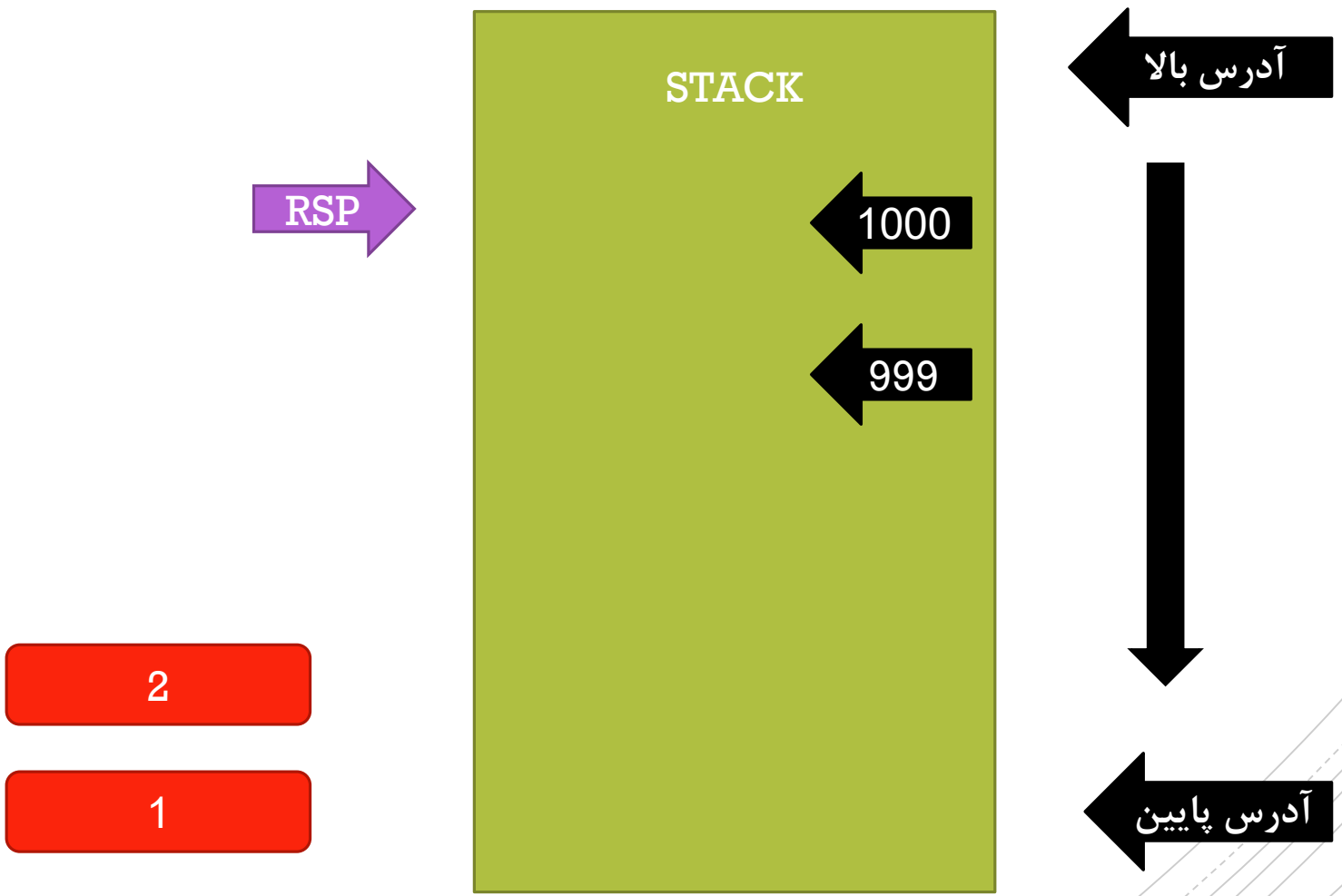
Github: Onhexgroup

پشته



Insta: Onhexgroup

پشته



Youtube: Onhexgroup

دستورات پشته

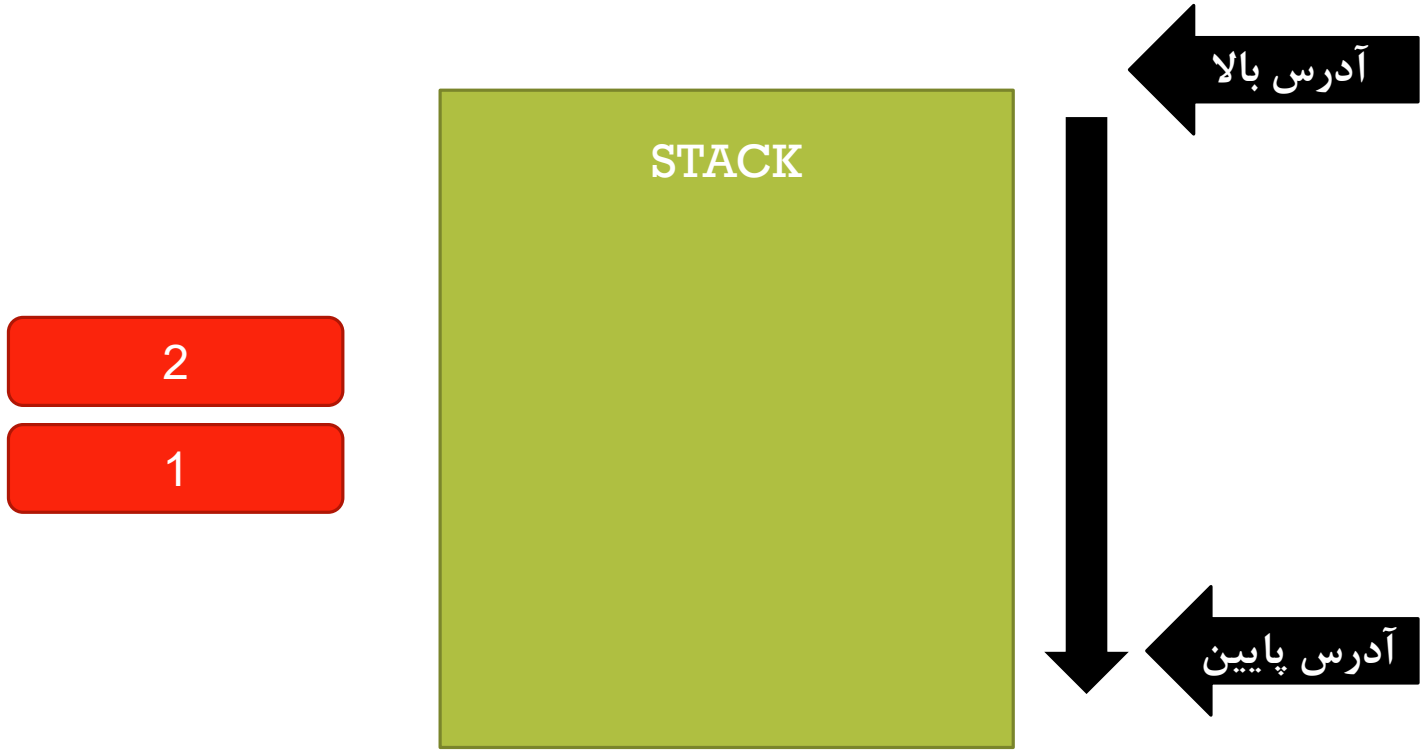
- برای قرار دادن در پشته از **PUSH** استفاده میکنیم.

PUSH R/M/IMM

نسخه	نوع عملوند	سایز پشته
۳۲ بیتی	مقدار صریح	۴ بایت کم میکند
	رجیستر	در حالت بایتی و **Dword** ۴ بایت و در حالت **WORD** ۲ بایت کم میکنن.
	موری	در حالت بایتی و **Dword** ۴ بایت و در حالت **WORD** ۲ بایت کم میکنن.
۶۴ بیتی	مقدار صریح	حالت **Qword** ممنوع. بقیه حالات ۸ بایت کم میکنن.
	رجیستر	حالت بایتی و **Dword** ممنوع. حالت **WORD** ۲ بایت حالت **QWORD** ۸ بایت
	موری	حالت بایتی و **Dword** ممنوع. حالت **WORD** ۲ بایت حالت **QWORD** ۸ بایت

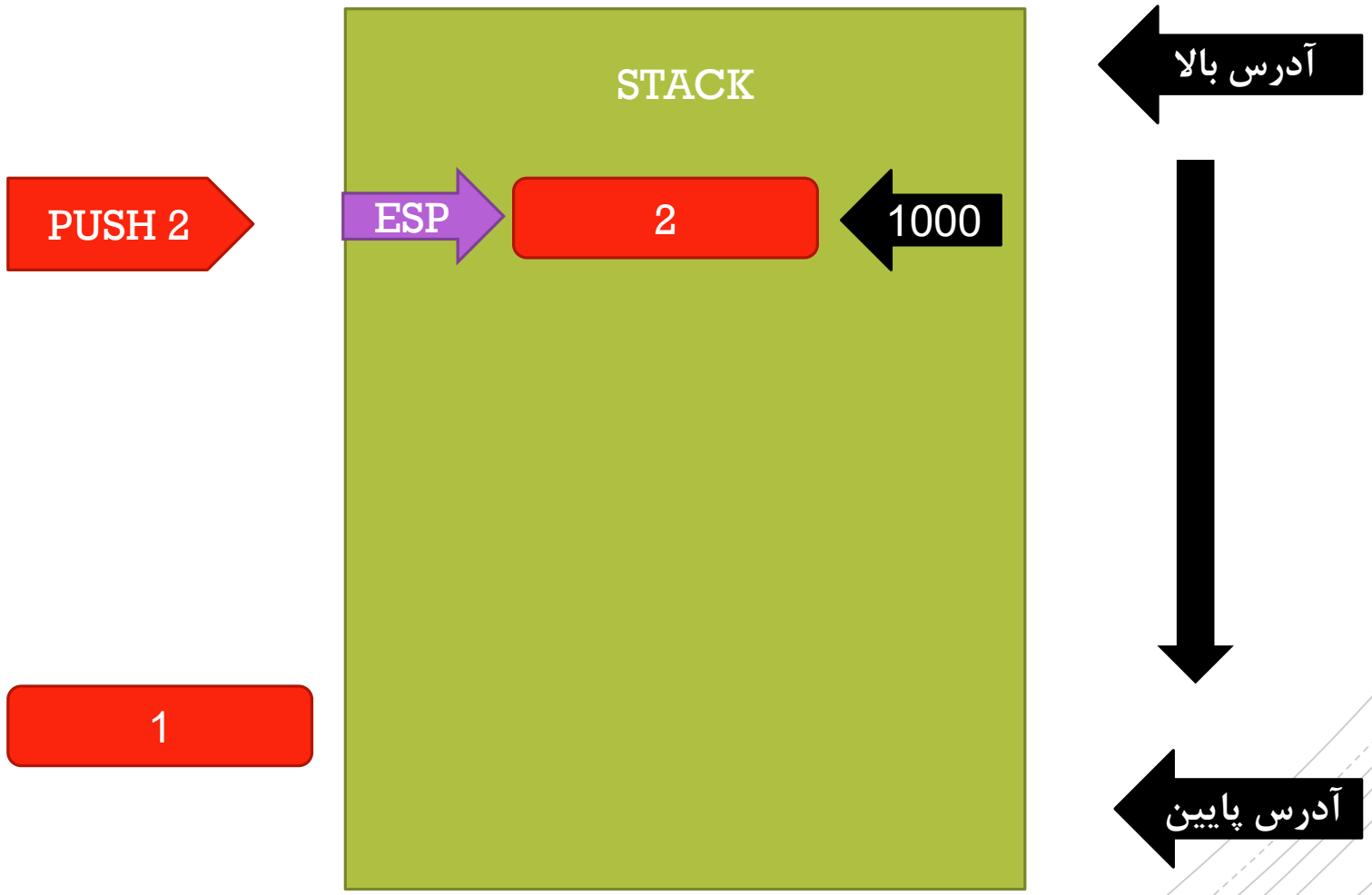
Youtube: Onhexgroup

دستورات پشته



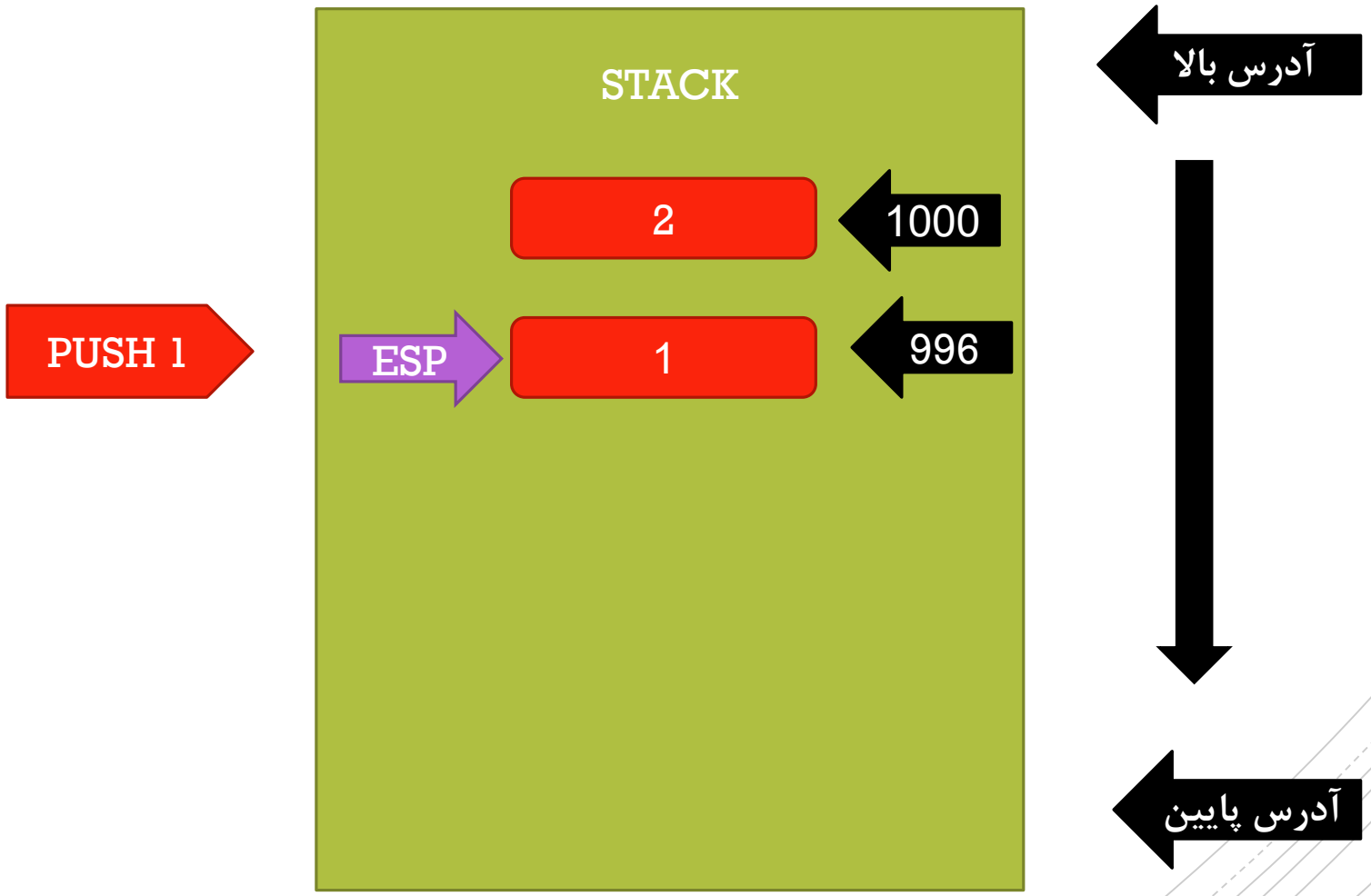
Onhexgroup.ir

پشته



Twitter: Onhexgroup

پشته



Github: Onhexgroup

دستورات پشته

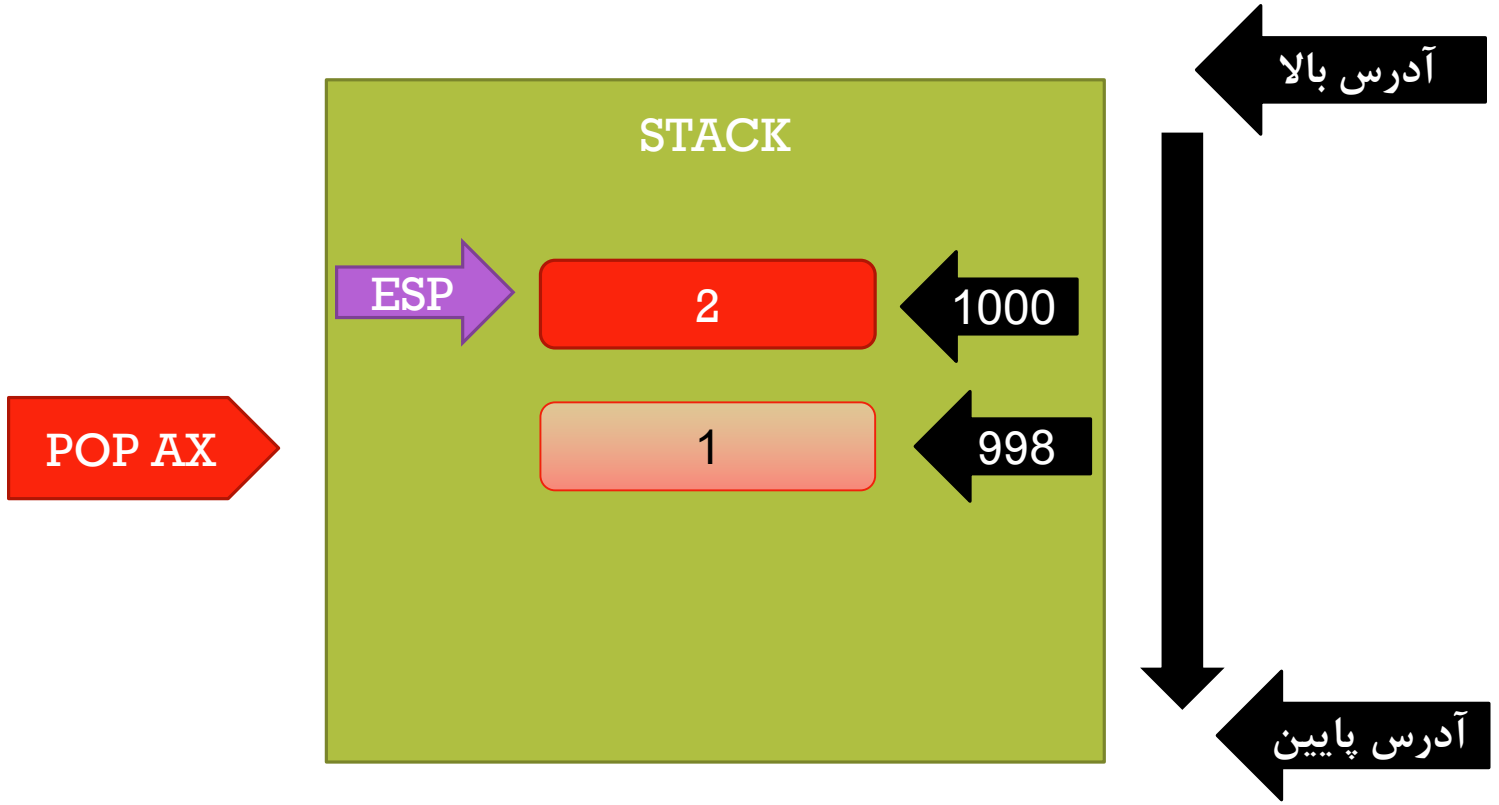
- برای برداشتن از پشته از **POP** استفاده میکنیم.

POP R/M

نسخه	نوع عملوند	سایز پشته
۳۲ بیتی	رجیستر	در حالت بایتی و **word** 2 بایت و در حالت **Dword** 4 بایت اضافه میکنن.
	موری	در حالت بایتی و **word** 2 بایت و در حالت **Dword** 4 بایت اضافه میکنن.
۶۴ بیتی	رجیستر	حالت بایتی و **Dword** ممنوع. حالت **WORD** ۲ بایت حالت **QWORD** ۸ بایت
	موری	حالت بایتی و **Dword** ممنوع. حالت **WORD** ۲ بایت حالت **QWORD** ۸ بایت

Github: Onhexgroup

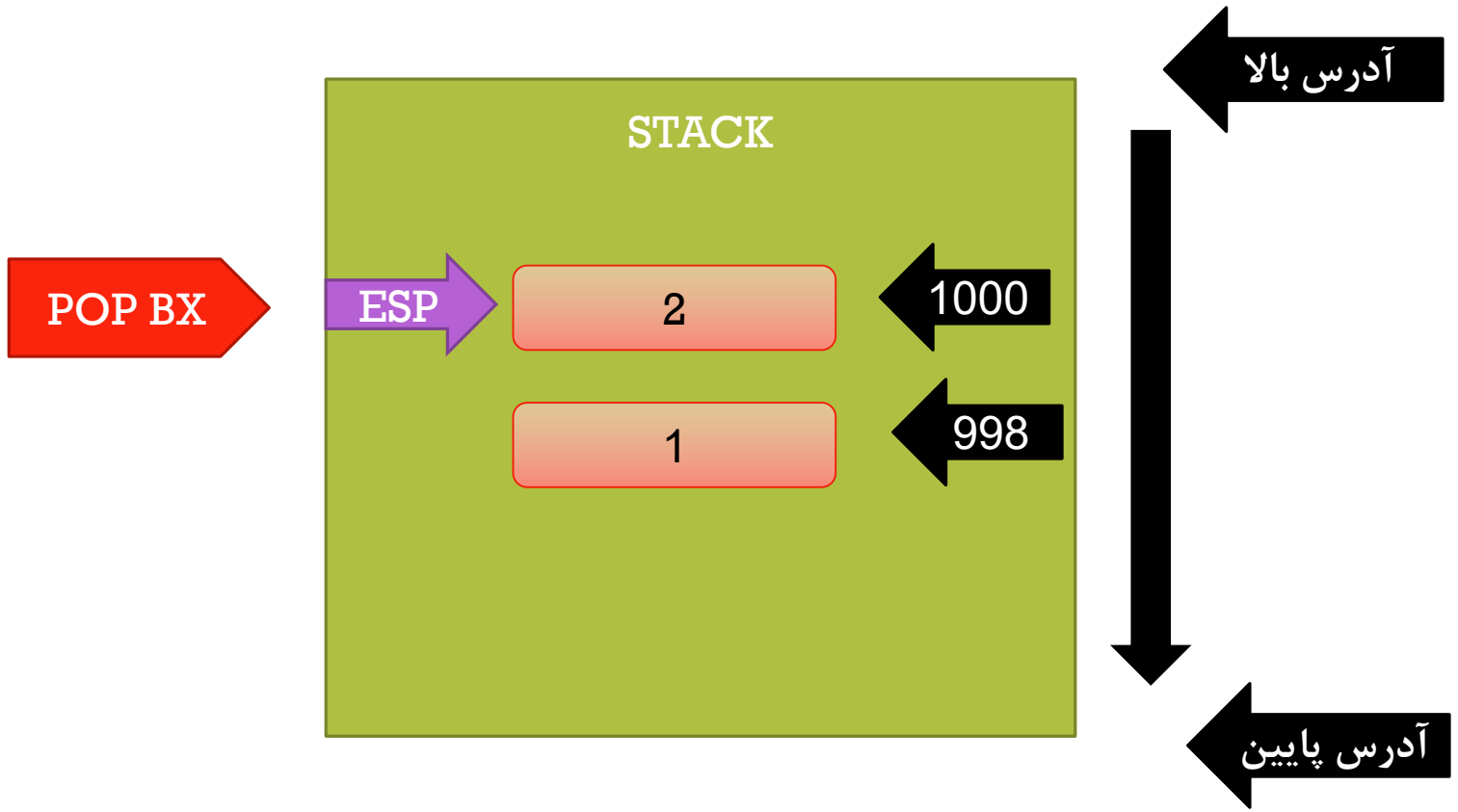
دستورات پشته



AX=1

Youtube: Onhexgroup

دستورات پشته



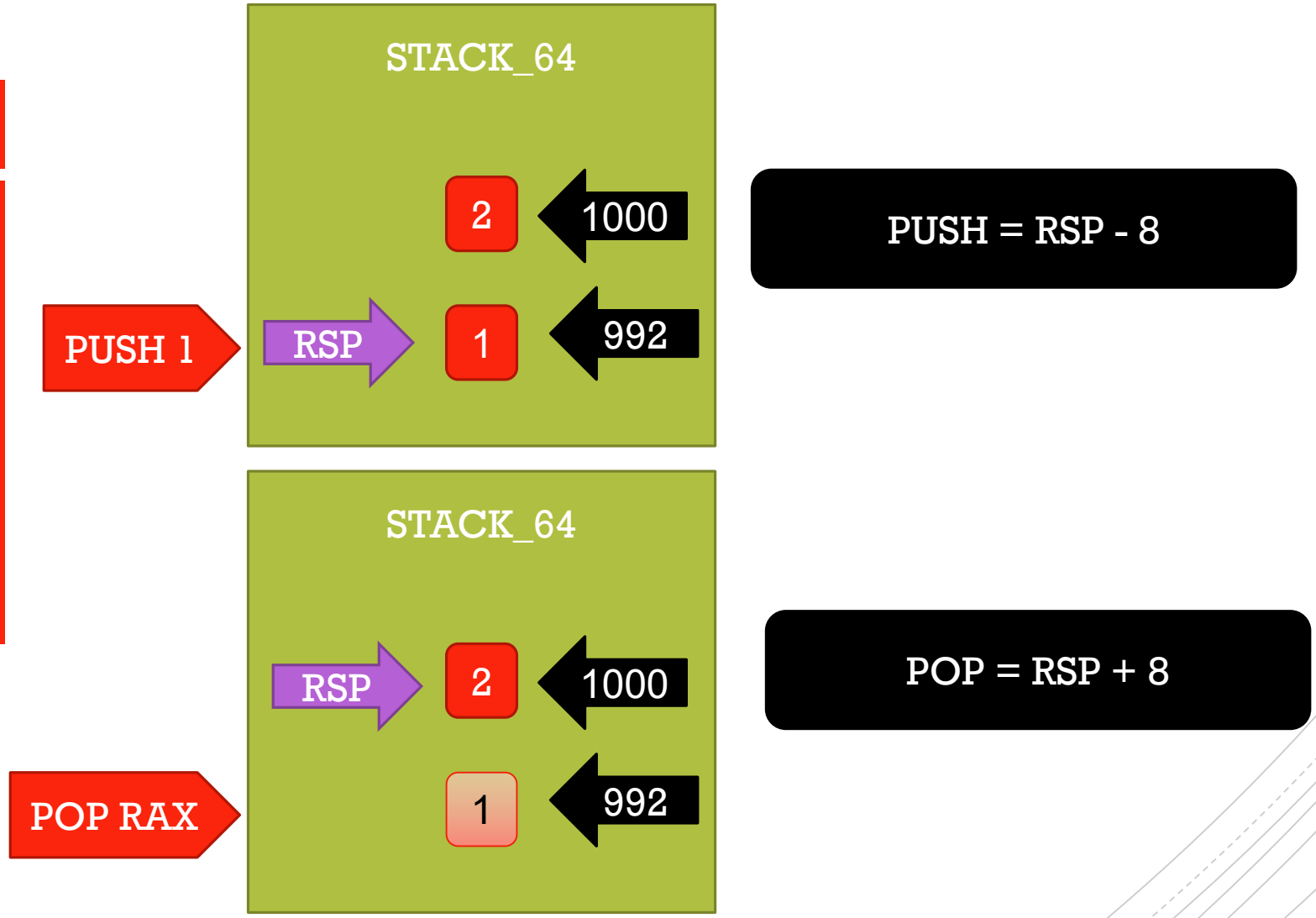
BX=2

AX=1

- دستورات **ADD** و **SUB** در پشته

Github: Onhexgroup

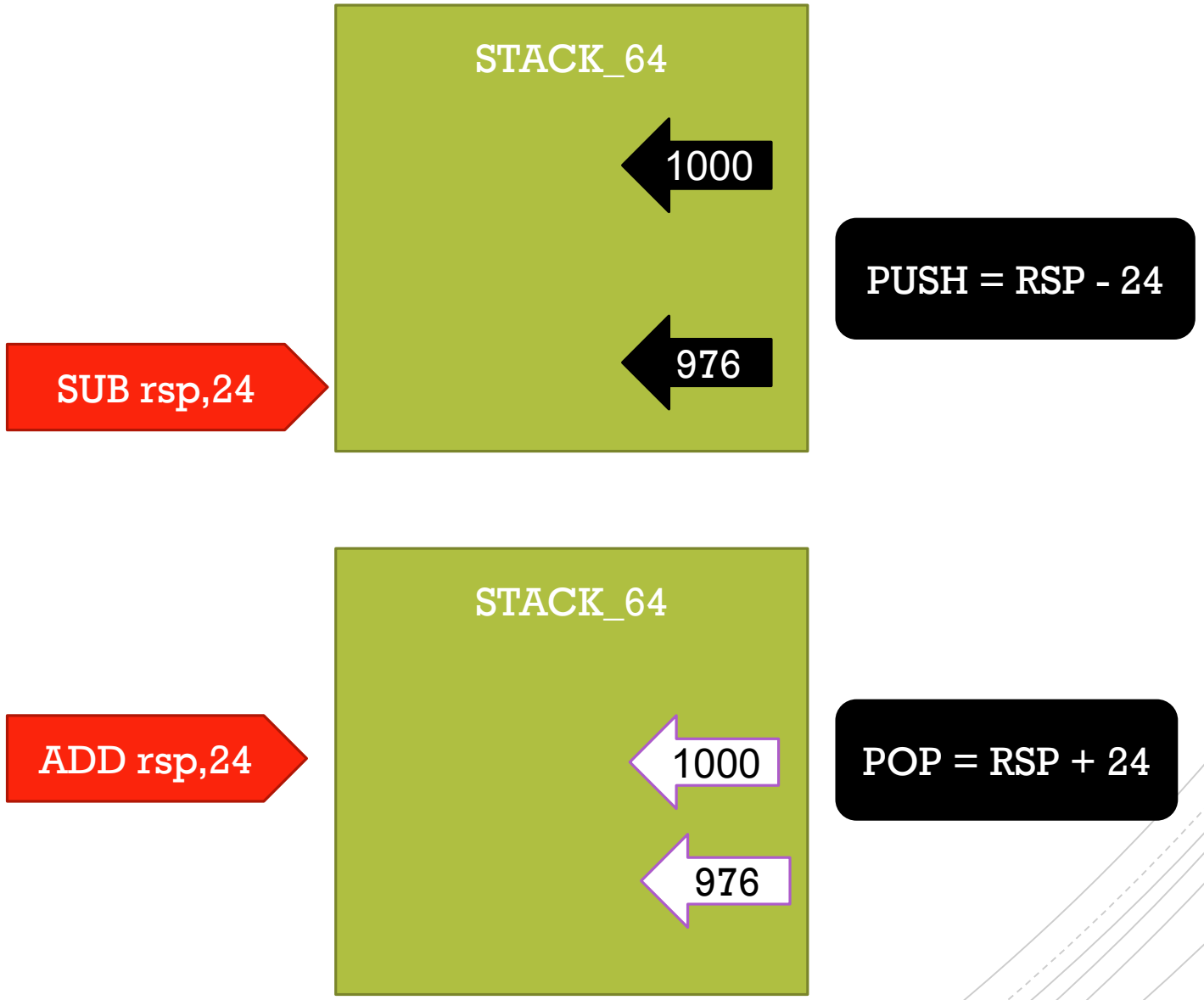
دستورات پشته



Youtube: Onhexgroup

دستورات پشته

دستورات ADD و SUB در پشته



Onhexgroup.ir

دستورات پشته

- دستورات **MOV** و **LEA** در پشته

MOV esp,[eax]

Lea eax,[rsp]

Youtube: Onhexgroup

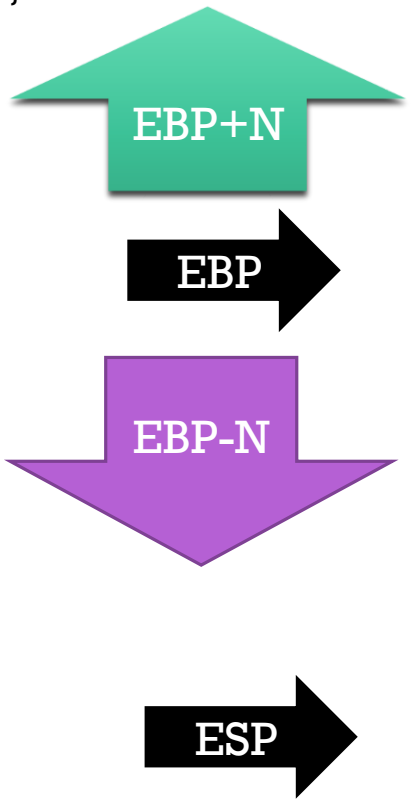
قاب پشته

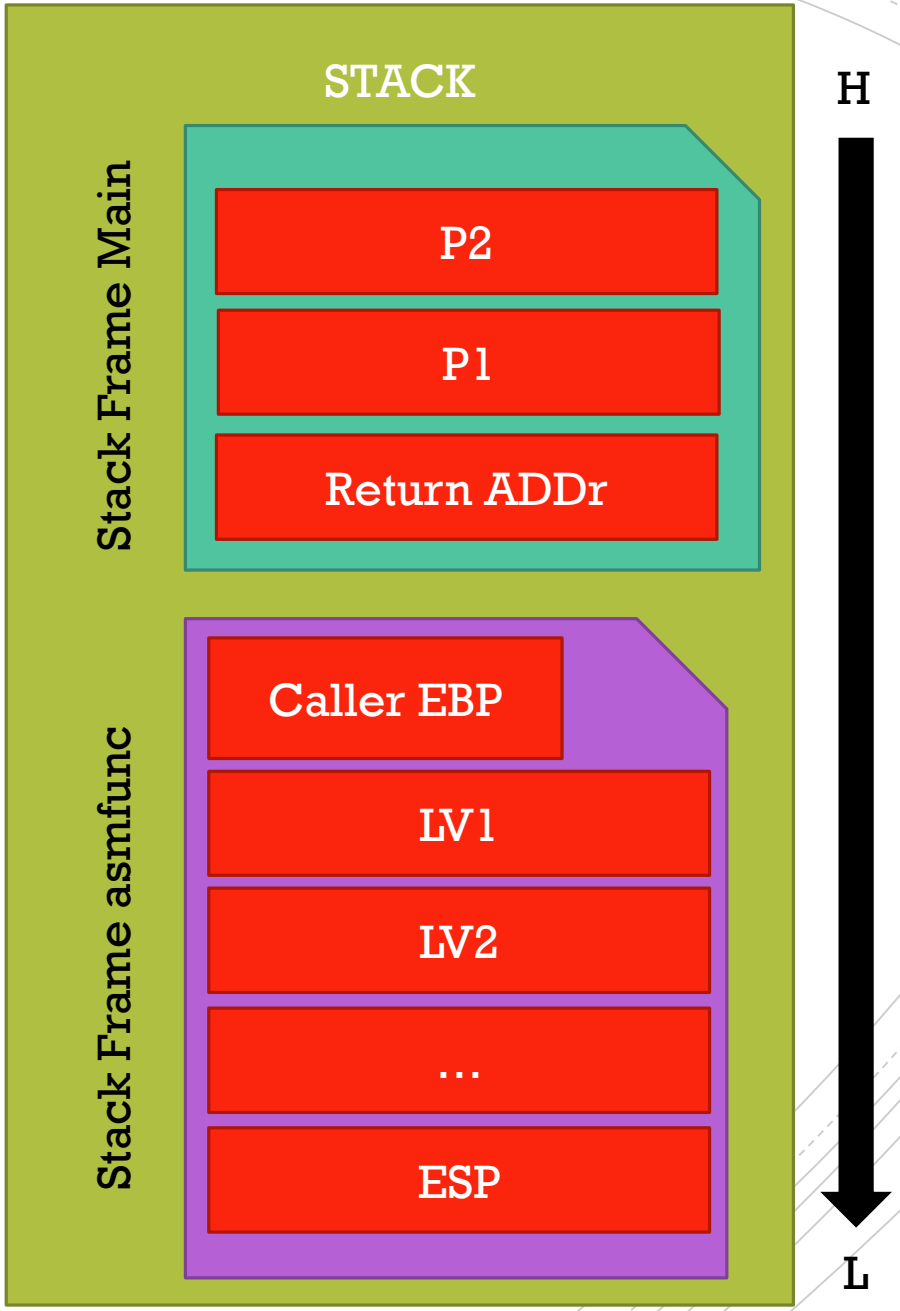
- قاب پشته یا فریم پشته یا **Stack frame**، بخشی از پشته که موقع فراخوانی تابع ایجاد میشه.
- این قاب شامل همه ی موارد مورد نیاز برای اجرای یک تابع و برگشت به نقطه قبل است.
- اشاره گر پایه (مرجع فریم): **EBP** یا **RBP**

Twitter: Onhexgroup

EBP/RBP

```
Void main(){
        asmfunc(P1,P2)
}
Void asmfunc(P1,P2){
        LV1;
        LV2;
}
```





Telegram: onhex_ir

درصد