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**

Onhexgroup.ir

دستورات پرش

- همیشه قرار نیست، روند اجرای برنامه به ترتیب و پشت سر هم از بالا به پایین باشه.
- مثلا در ساختار تصمیم، حلقه ها و ... .
- انواع دستورات پرشی:
  - دستورات پرش غیر شرطی
  - دستورات پرش شرطی

```
B=2
A= user_input
If(a>b):
        Print(“BOZORG AST”)
Elseif(b>a):
        Print(“KUCHAK AST”)
Esleif(a=b):
        Print(“MOSAVI AST”)
```

Youtube: Onhexgroup

دستور پرش غیر شرطی

- پرش بدون هیچ شرطی
- عملکردش:

JMP ADDR_Where

شکل **RM** :

JMP IMM/R/M

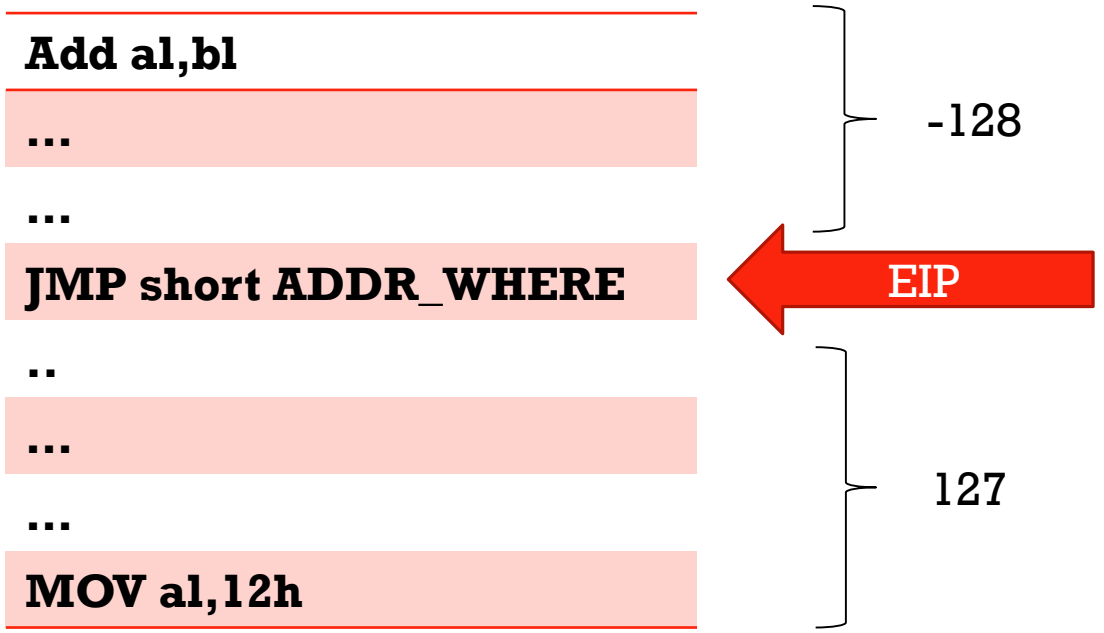
- روی فلگها تاثیر نداره.
- انواع دستور **JMP**:

- **Short**
- **NEAR**
- **FAR**
- **Task Switch**

- پرش در محدوده بین ۱۲۸- تا ۱۲۷ بایت از EIP
- سایز ۲ بایت

Github: Onhexgroup

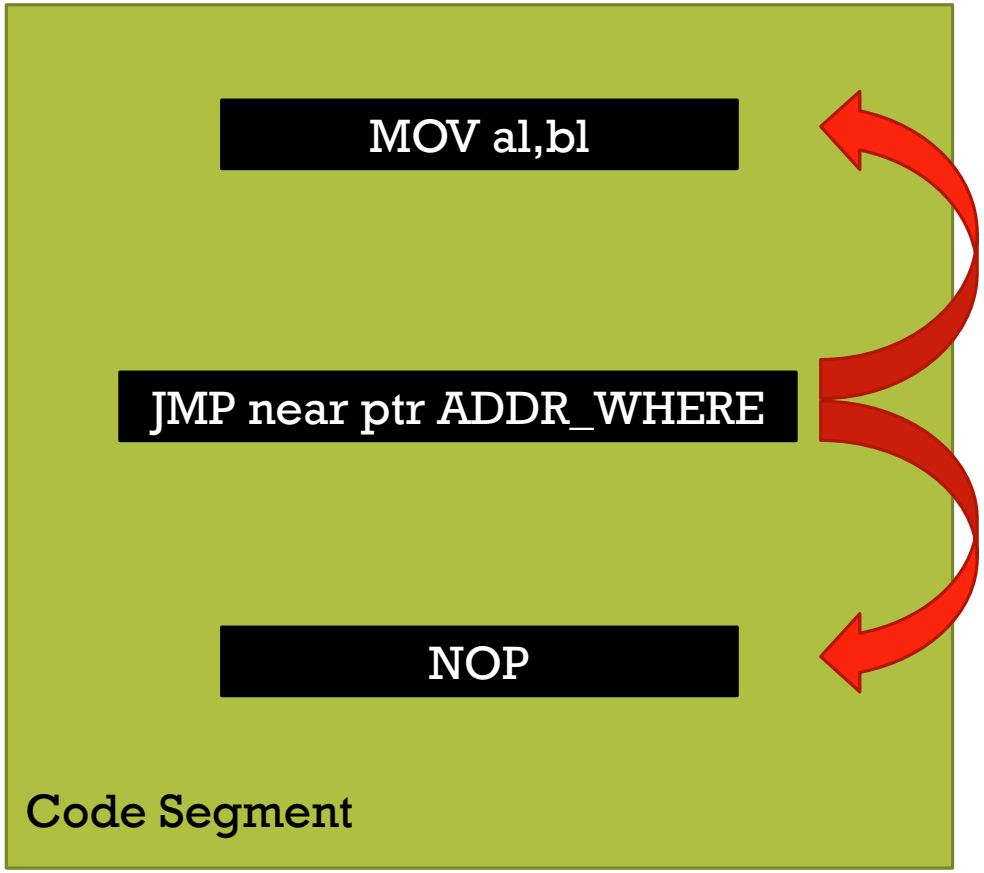
Short Jump



Twitter: Onhexgroup

Near Jump

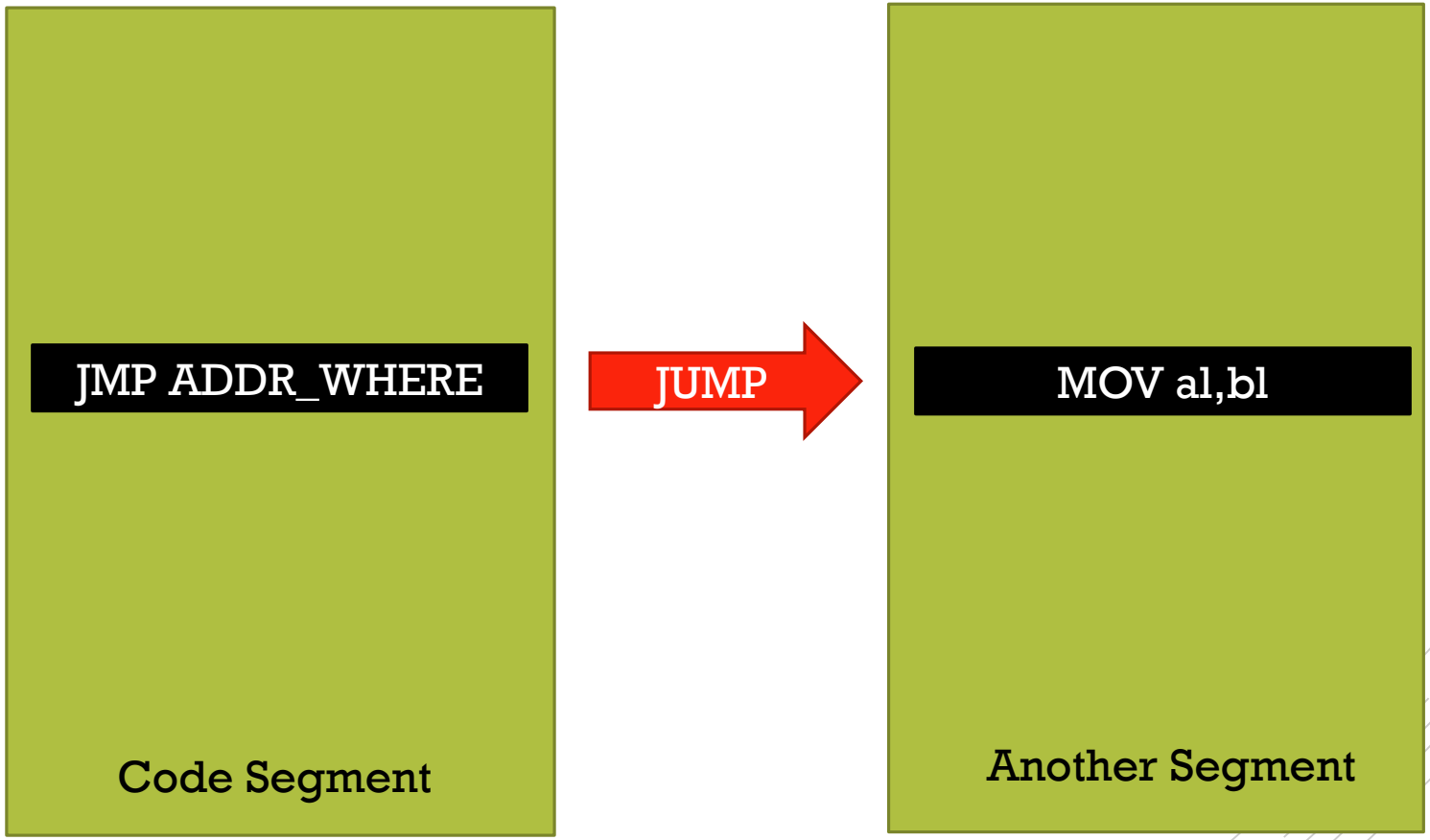
- پرش به یک دستور العمل در سگمنت کد فعلی – سگمنتی که توسط رجیستر **CS** بهش اشاره میشه.
- سایز ۵ بایت



- پرش به دستورالعملی که در سگمنت دیگه از سگمنت کد و با همون سطح دسترسی **(Privilege Level)** قرار داره.
- سایز ۶ بایت

Instagram: Onhexgroup

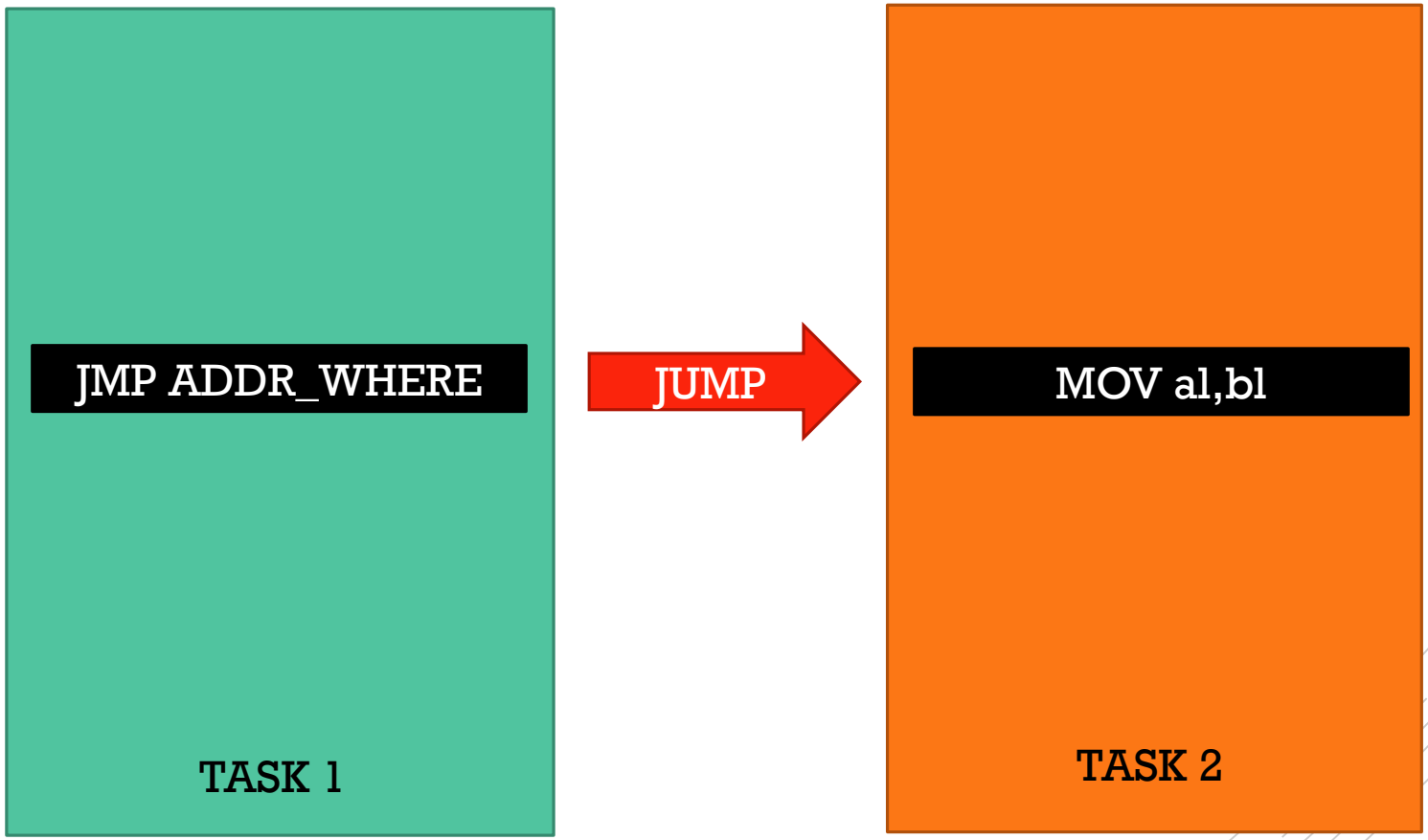
Far Jump



- پرش به تسک دیگه در سیستم های **Multitasking** – تعویض تسک
- سایز متغیر

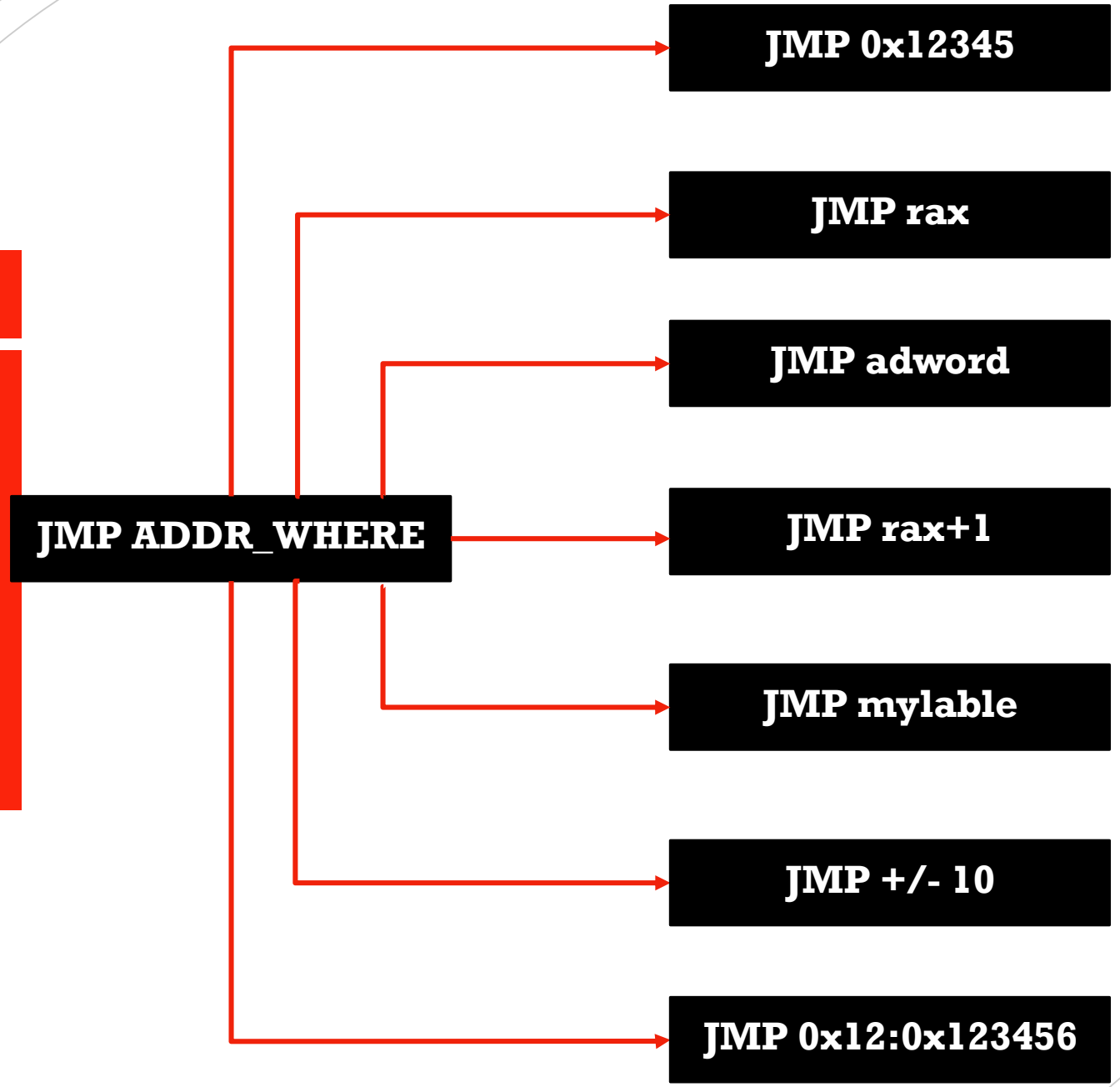
Onhexgroup.ir

Task Switch



Youtube: Onhexgroup

نوع آدرس



Github: Onhexgroup

دستورات پرش شرطی

- پرش براساس شرایط و وضعیت
- وضعیت = **EFLAG** و **RFLAG**
- دستورات اسمبلی که روی فلگ ها تاثیر میزارن:
- **CMP (CF, OF, SF, ZF, AF, PF)**
- **TEST(OF, CF, SF, ZF, PF)**

Instagram: Onhexgroup

نشانه ها در دستورات پرش شرطی

عبارت	نشانه
JUMP	J
ABOVE	A
Equal	E
Below	B
Carry	C
Greater	G
Less	L
NOT	N
Overflow	O
Parity	P
Sign	S
ZERO	Z
CX Register	CX
ECX Register	ECX
RCX Register	RCX

Twitter: Onhexgroup

دستورات پرش شرطی

دستور	مفهوم	وضعیت
JA	بپر اگه بیشتر بود.	CF and ZF = 0
JNA	بپر اگه بیشتر نبود	CF OR ZF = 1
JAE	بپر اگه بیشتر یا مساوی بود	CF=0
JNAE	بپر اگه بیشتر یا مساوی نبود	CF=1
JB	بپر اگه کمتر بود	CF=1
JNB	بپر اگه کمتر نبود	CF=0
JBE	بپر اگه کوچکتر یا مساوی بود	ZF OR CF=1
JNBE	بپر اگه کوچکتر یا مساوی نبود	ZF AND CF=0
JC	بپر اگه Carry بود	CF=1
JNC	بپر اگه Carry نبود	CF=0
JCX	بپر اگه CX صفر بود	CX=0
JECX	بپر اگه ECX صفر بود	ECX=0
JRCX	بپر اگه RCX صفر بود	RCX=0

Telegram: onhex_ir

دستورات پرش شرطی

دستور	مفهوم	وضعیت
JE	بپر اگه مساوی بود	ZF=1
JNE	بپر اگه مساوی نبود	ZF=0
JG	بپر اگه بزرگتر بود	ZF and SF=0
JNG	بپر اگه بزرگتر نبود	ZF=1 OR SF ≠ OF
JGE	بپر اگه بزرگتر یا مساوی بود	SF=OF
JNGE	بپر اگه بزرگتر یا مساوی نبود	SF ≠ OF
JL	بپر اگه کوچکتر بود	SF ≠ OF
JNL	بپر اگه کوچکتر نبود	SF=OF
JLE	بپر اگه کوچکتر یا مساوی بود	ZF=1 or SF ≠ OF
JNLE	بپر اگه کوچکتر یا مساوی نبود	SF=OF
JO	بپر اگه overflow بود	OF=1
JNO	بپر اگه overflow نبود	OF=0
JZ	بپر اگه صفر بود	ZF=1
JNZ	بپر اگه صفر نبود	ZF=0

Onhexgroup.ir

دستورات پرش شرطی

دستور	مفهوم	وضعیت
JS	بپر اگه Sign بود	SF=1
JNS	بپر اگه Sign نبود	SF=0
JP	بپر اگه Parity بود	PF=1
JNP	بپر اگه Parity نبود	PF=0
JPE	بپر اگه زوج بود	PF=1
JPO	بپر اگه فرد بود	PF=0

Telegram: onhex_ir

درصد

ONHEXGROUP

69%

NOP 10%	PUSH 15%	CALL 8%	LEA 5%
MOV 27%	INT3 5%	ADD 3%	JNZ 2%
POP 3%	JMP 2%	XOR 2%	XADD 1%
CMP 3%	JG 1%	DEC 1%	JZ 2%
TEST 3%	RET 2%	SUB 2%	OTHRES 5%