

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**

■ رجیسترها حافظه های سریعی هستند و مانند یک متغیر عمل میکنند

Onhexgroup.ir

مفهوم رجیسترها

A=1



B=3

Twitter:Onhexgroup

مفهوم رجیسترها

A=1



B=3

CPU



A=?

B=?

Twitter:Onhexgroup

مفهوم رجیسترها

A=1



B=3

CPU



A=?

B=?

e

3

f

1

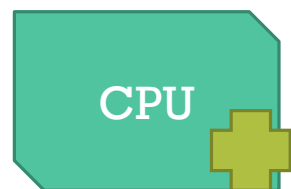
Twitter:Onhexgroup

مفهوم رجیسترها

A=1



B=3



A=?

1

3

B=?

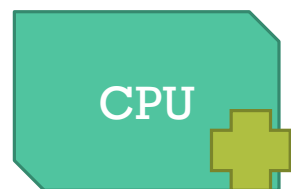
Twitter:Onhexgroup

مفهوم رجیسترها

A=1



B=3



A=?

B=?

0 1 2 3

1 3

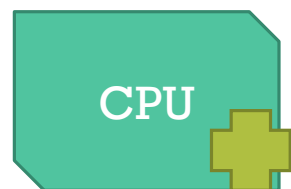
Twitter:Onhexgroup

مفهوم رجیسترها

A=1



B=3



A=?

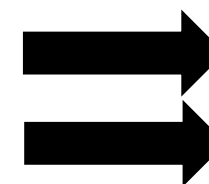
EAX

1

EBX

3

B=?



Telegram: onhex_ir

انواع رجیسترهای پایه

- رجیسترهای همه منظوره
- رجیسترهای سگمنت
- رجیسترهای وضعیت و کنترلی
- رجیستر اشاره گر دستور

Youtube: @onhexgroup

رجیسترهای همه منظوره

- رجیسترهای همه منظوره یا رجیسترهای عمومی یا General Purpose register یا GPR
- امکان استفاده در همه جا و قابلیت ذخیره داده و آدرس دارن
- البته کاربردهای خاصی رو هم دارن

Github: @onhexgroup

رجیسترهای همه منظوره

■ در سیستم های ۳۲ بیتی :

■ اندازه رجیسترها حداکثر ۳۲ بیت

■ ۸ رجیستر همه منظوره داریم:

■ **EAX , EBX , ECX , EDX , ESI , EDI , EBP , ESP**

■ در سیستم های ۶۴ بیتی :

■ اندازه رجیسترها حداکثر ۶۴ بیت

■ ۱۶ رجیستر همه منظوره داریم :

■ **RAX,RBX,RCX,RDX,RSI,RDI,RBP,RSP,R8...R15**

■ **R0...R15**

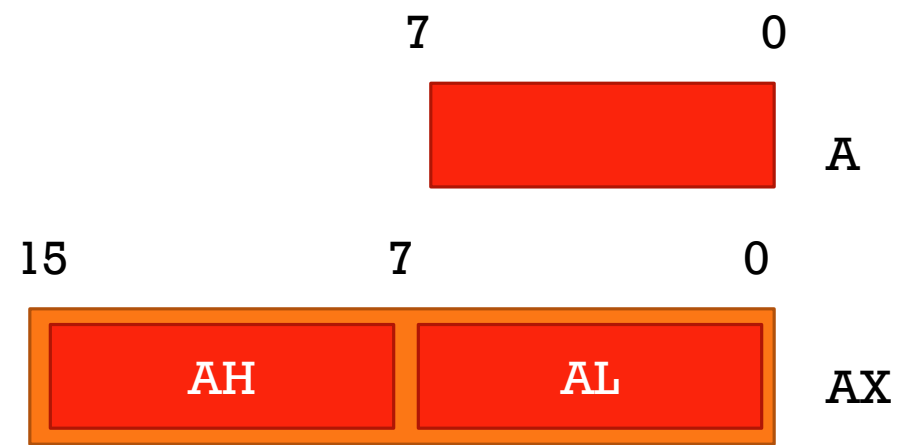
Onhexgroup.ir

اندازه رجیسترهای
همه منظوره

7 0
A

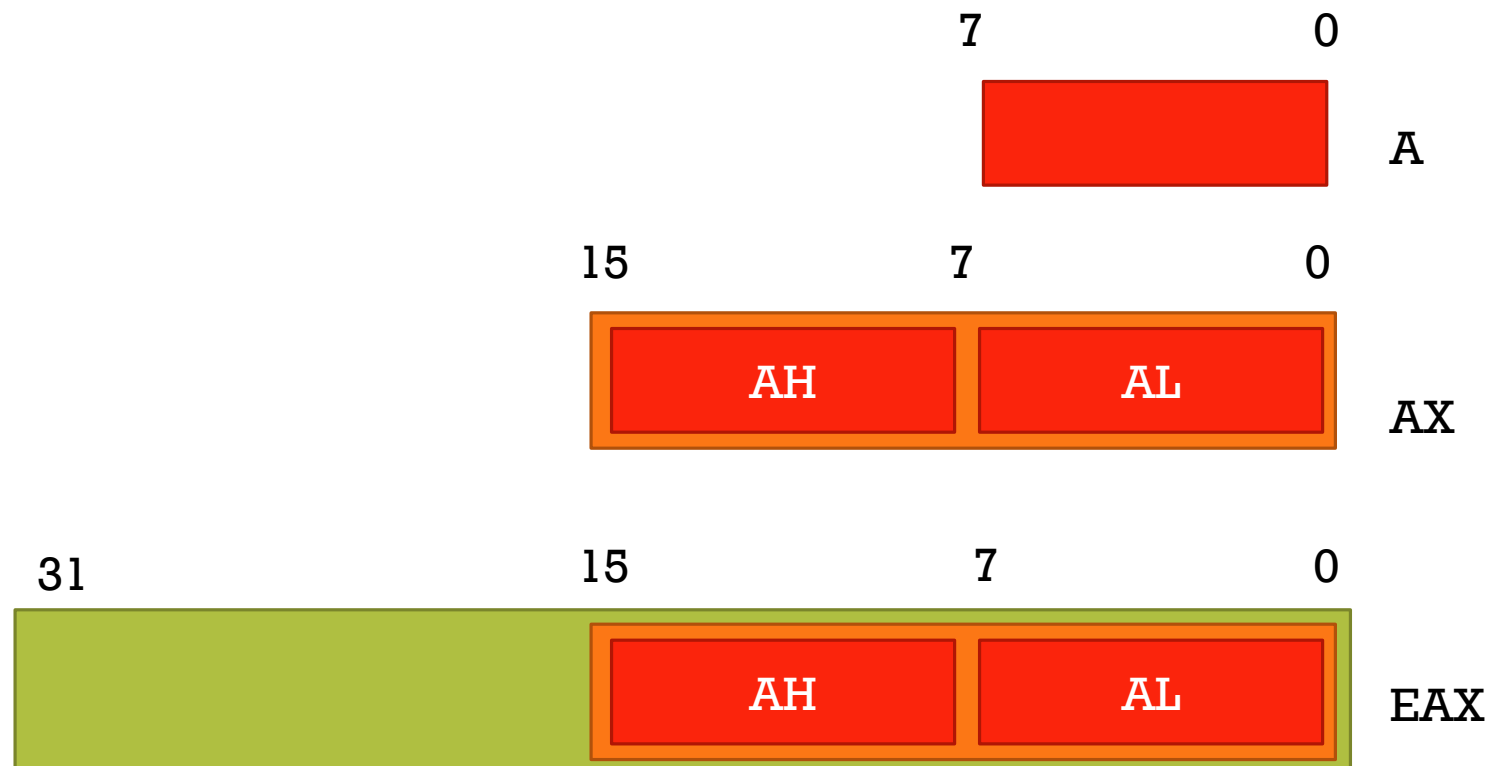
Telegram: onhex_ir

اندازه رجیسترهای
همه منظوره



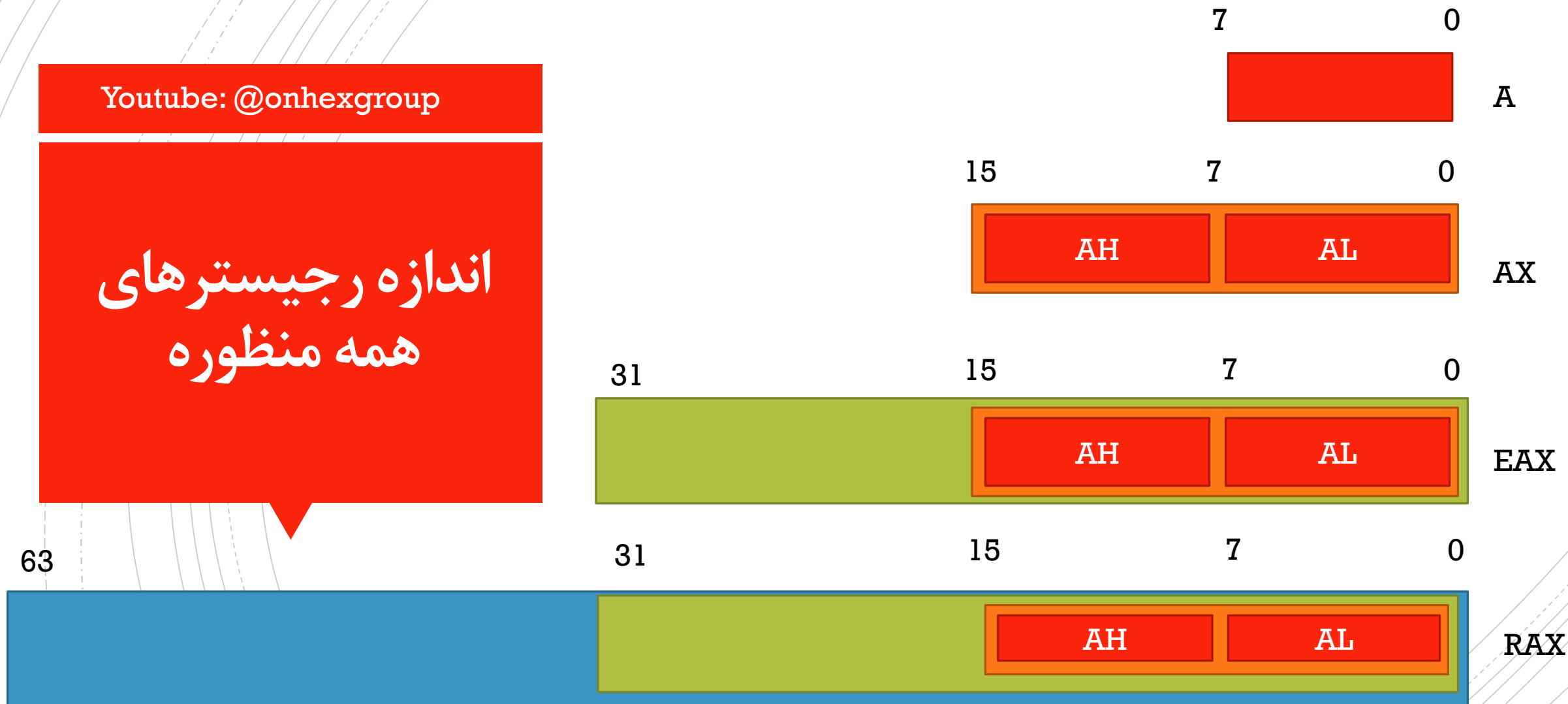
Youtube: @onhexgroup

اندازه رجیسترهای
همه منظوره



Youtube: @onhexgroup

اندازه رجیسترهای
همه منظوره



Github: @onhexgroup

نوع داده رجیسترهای همه منظوره

■ رجیستر **AL** و **AH** = ۸ بیت = ۱ بایت

■ رجیستر **AX** = ۱۶ بیت = ۲ بایت = ۱ کلمه

■ رجیستر **EAX** = ۳۲ بیت = ۴ بایت = ۲ کلمه = ۱ **Dword**

■ رجیستر **RAX** = ۶۴ بیت = ۸ بایت = ۴ کلمه = ۲ **DWORD** = ۱ **QWORD**

Youtube: @onhexgroup

اندازه رجیسترهای
همه منظوره
در ۶۴ بیتی

7 0

R0B

Byte

15 7 0

R0W

Word

31 15 7 0

R0D

DWord

63

31 15 7 0

RAX – R0

QWord

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : EAX

■ در ۶۴ بیتی : RAX یا R0

■ انباره یا Accumulator

Twitter: @onhexgroup

رجیستر
EAX/RAX/R0

AH or R0H

AL - R0B - R0L

AX or R0W

EAX or R0D

RAX or R0

63

31

15

7

0

■ رجیستر همه منظوره هستش.

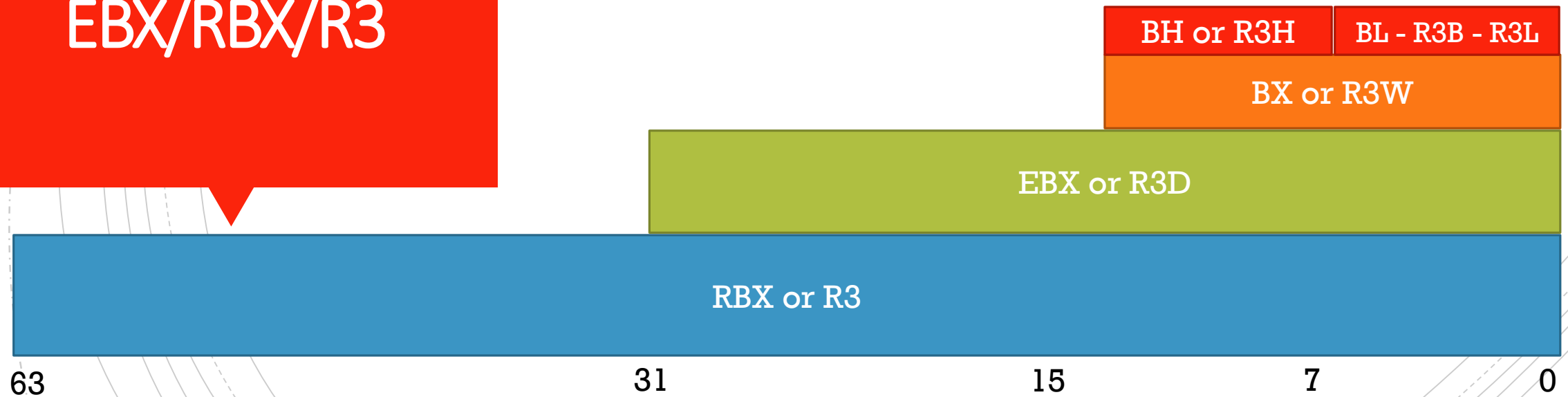
■ در ۳۲ بیتی : EBX

■ در ۶۴ بیتی : RBX یا R3

■ Base Register : آدرس Base برنامه رو ذخیره میکنه.

Youtube: @onhexgroup

رجیستر
EBX/RBX/R3



■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : ECX

■ در ۶۴ بیتی : RCX یا R1

■ شمارنده (Counter) برای رشته ها و حلقه ها

Github: @onhexgroup

رجیستر
ECX/RCX/R1

CH or R1H

CL - R1B - R1L

CX or R1W

ECX or R1D

RCX or R1

63

31

15

7

0

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : EDX

■ در ۶۴ بیتی : RDX یا R2

■ Data register و در عملیات I/O استفاده میشه.

OnHexGroup.ir

رجیستر
EDX/RDX/R2

DH or R2H

DL – R2B – R2L

DX or R2W

EDX or R2D

RDX or R2

63

31

15

7

0

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : ESP

■ در ۶۴ بیتی : RSP یا R4

■ اشاره گر پشته یا Stack pointer

Twitter: @onhexgroup

رجیستر
ESP/RSP/R4

فقط در ۶۴ بیتی در دسترس هست

SPL – R4B – R4L

SP or R4W

ESP or R4D

RSP or R4

63

31

15

7

0

Twitter: @onhexgroup

رجیستر
EBP/RBP/R5

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : EBP

■ در ۶۴ بیتی : RBP یا R5

■ اشاره گر به داده در پشته یا Base pointer – به انتهای فریم پشته اشاره میکنه

فقط در ۶۴ بیتی در دسترس هست

BPL – R5B – R5L

BP or R5W

EBP or R5D

RBP or R5

63

31

15

7

0

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : ESI

■ در ۶۴ بیتی : RSI یا R6

■ اشاره گر به داده و در عملیات رشته معروف Source Index

Twitter: @onhexgroup

رجیستر
ESI/RSI/R6

فقط در ۶۴ بیتی در دسترس هست

SIL – R6B – R6L

SI or R6W

ESI or R6D

RSI or R6

63

31

15

7

0

■ رجیستر همه منظوره هستش.

■ در ۳۲ بیتی : EDI

■ در ۶۴ بیتی : RDI یا R7

■ اشاره گر به داده و در عملیات رشته معروف به Destination Index

Twitter: @onhexgroup

رجیستر
EDI/RDI/R7

فقط در ۶۴ بیتی در دسترس هست

DIL – R7B – R7L

DI or R7W

EDI or R7D

RDI or R7

63

31

15

7

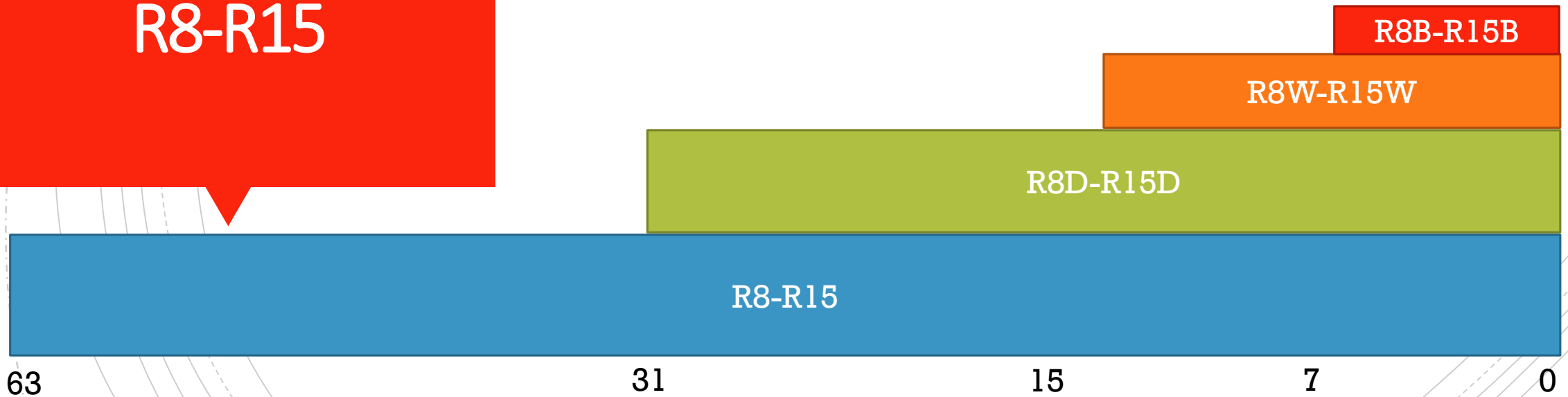
0

■ رجیستر همه منظوره ی جدید که مختص نسخه ی ۶۴ بیتی هستش.

■ از R8 تا R15 در دسترس هستن.

Twitter: @onhexgroup

رجیسترهای
R8-R15



■ سگمنت ناحیه ی پیوسته ای از مموری هستش که با آدرس شروع (Base) و محدوده تعریف میشه.

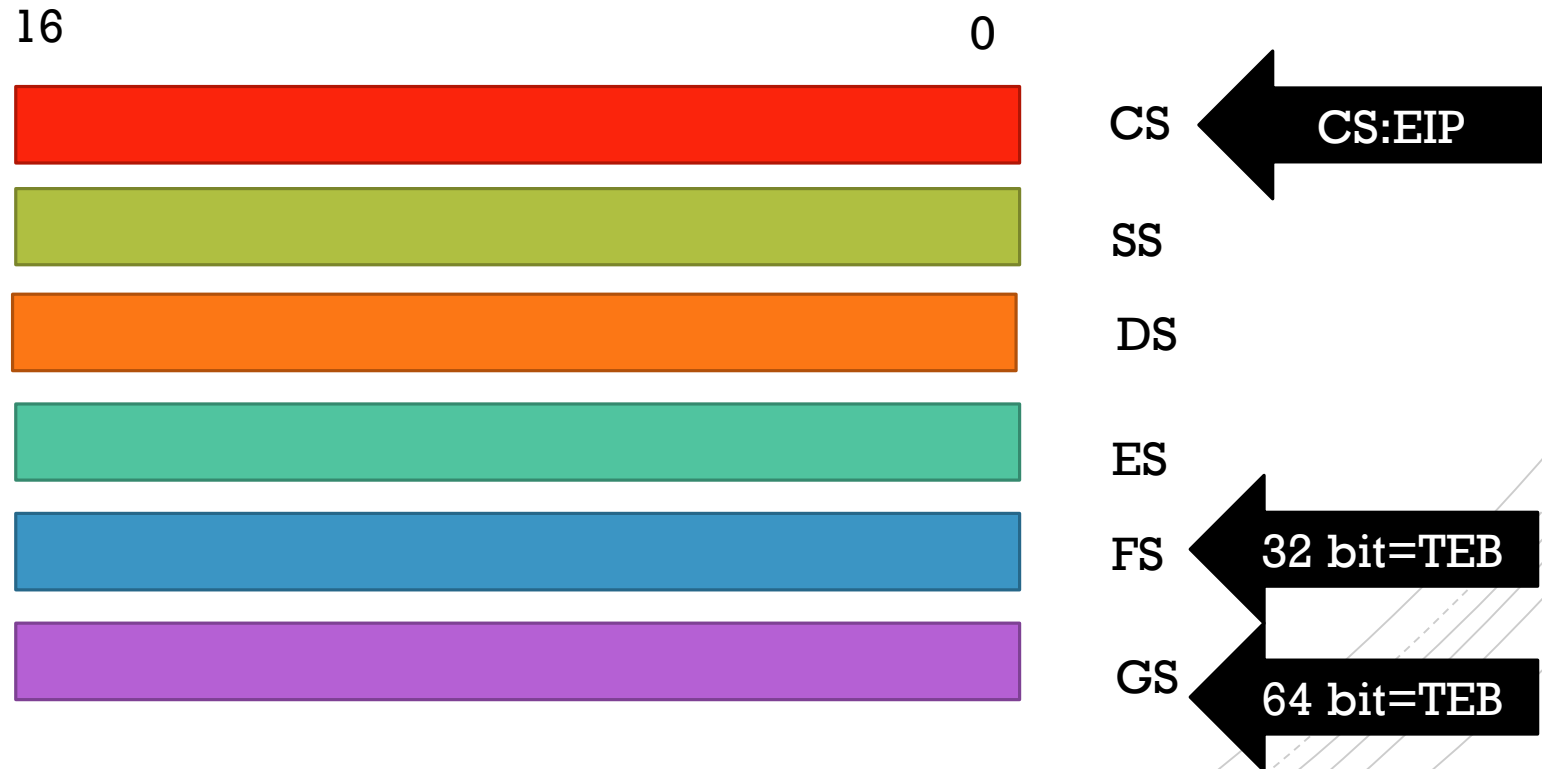
■ هدف : تقسیم حافظه برای حفاظت و کنترل ساده بود.

■ رجیسترهای سگمنت به این ناحیه ها اشاره میکنن.

■ این رجیسترها در سیستم های مدرن زیاد استفاده نمیشن. (مدل Flat)

■ در کل ۶ تا رجیستر سگمنت داریم که هر کدوم به یه بخشی از حافظه اشاره میکنن (محل شروع) :

رجیسترهای سگمنت



■ هر بیتش یه نامی داره که بهش فلگ میگن.

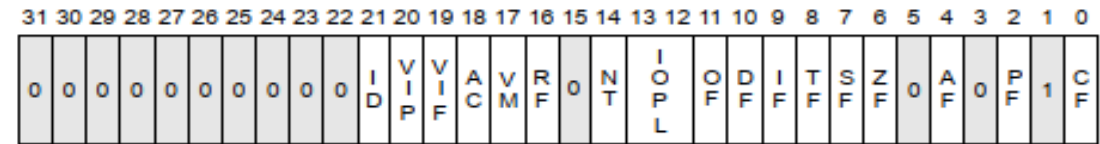
■ در ۳۲ بیتی اندازه اش ۳۲ بیت

■ در ۶۴ بیتی اندازه اش ۶۴ بیت

■ فلگ های سیستمی ، کنترلی و وضعیتی

Twitter: @onhexgroup

رجیسترهای وضعیت و کنترلی EFLAGS/RFLAGS



- X ID Flag (ID)
- X Virtual Interrupt Pending (VIP)
- X Virtual Interrupt Flag (VIF)
- X Alignment Check / Access Control (AC)
- X Virtual-8086 Mode (VM)
- X Resume Flag (RF)
- X Nested Task (NT)
- X I/O Privilege Level (IOPL)
- S Overflow Flag (OF)
- C Direction Flag (DF)
- X Interrupt Enable Flag (IF)
- X Trap Flag (TF)
- S Sign Flag (SF)
- S Zero Flag (ZF)
- S Auxiliary Carry Flag (AF)
- S Parity Flag (PF)
- S Carry Flag (CF)

- S Indicates a Status Flag
- C Indicates a Control Flag
- X Indicates a System Flag

■ Reserved bit positions. DO NOT USE.
Always set to values previously read.

Twitter: @onhexgroup

رجیستر
اشاره گر آدرس
EIP/RIP

■ Instruction Pointer Register

■ نشون دهنده آدرس بعدی که میخواد اجرا بشه

■ برنامه مستقیما نمیتونه تغییرش بده

■ در ۳۲ بیتی ، ۳۲ بیت و در ۶۴ بیتی ، ۶۴ بیت اندازه داره

Twitter: @onhexgroup

مصادر

- <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/x86-architecture>
- <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/x64-architecture>
- https://en.wikibooks.org/wiki/X86_Assembly/X86_Architecture