

ReverseCraft

assembler by gynvael.coldwind//vx

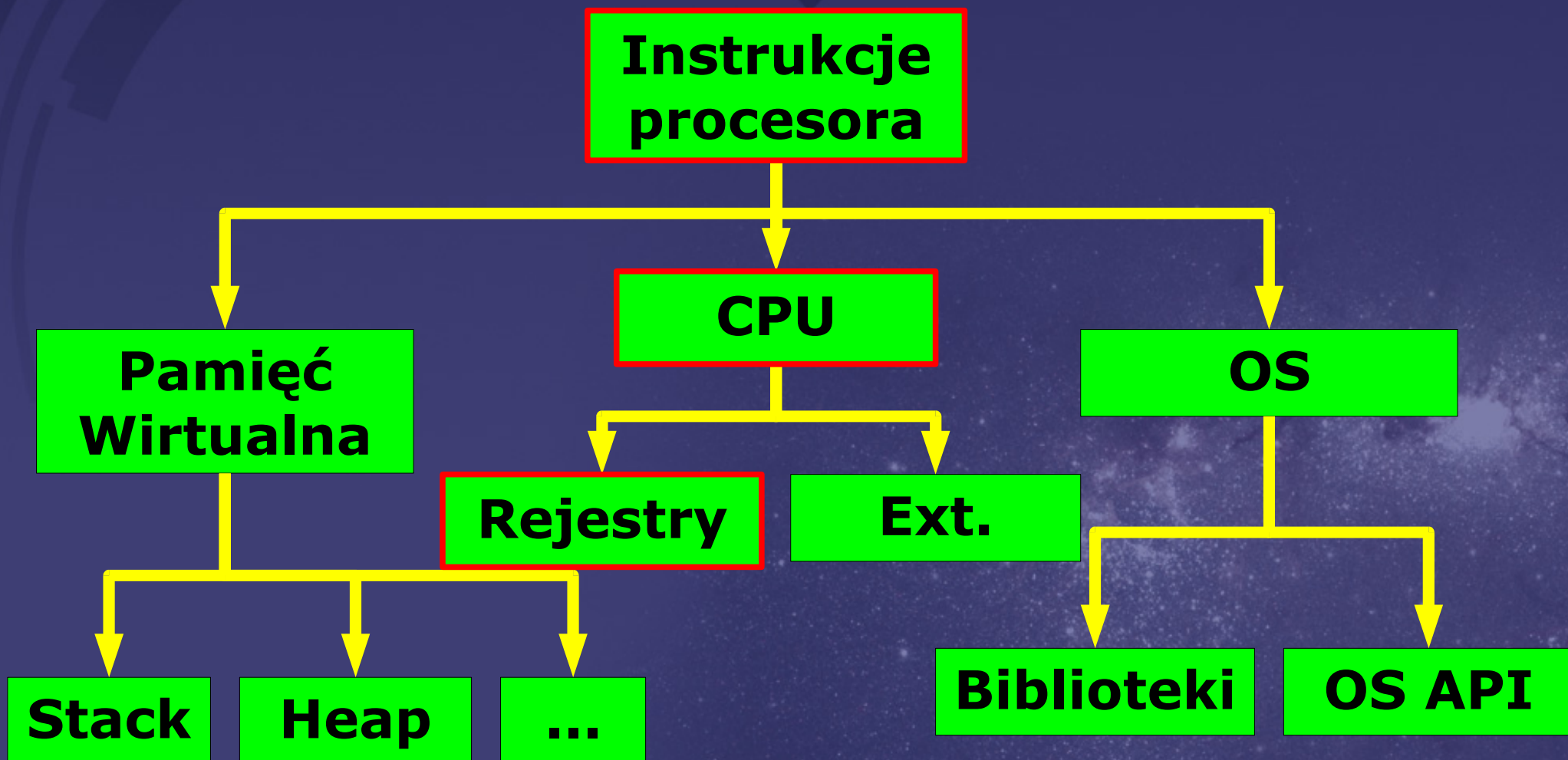
003 - EFLAGS, skoki

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>

Zasoby!

czyli co możemy użyć...



Flagi ?

W zasadzie, to wartość typu bool (true/false)

Po co flagi ?

**Żeby zachować odpowiedź na pytanie
czy coś miało miejsce**

**Żeby określać zachowanie pewnych obiektów
w przyszłości**

EFLAGS

Instrukcje arytmetyczno-logiczne ustawiają flagi, w zależności od wyniku operacji.

Część flag to flagi systemowe lub sterujące zachowaniami pewnych instrukcji.

Niektórych flag nie można zmienić ani odczytać w prosty sposób (np. RF).

Inne można zarówno zmieniać jak i odczytywać na kilka sposobów.

Intel Manuals, tom 1, rysunek 3-8

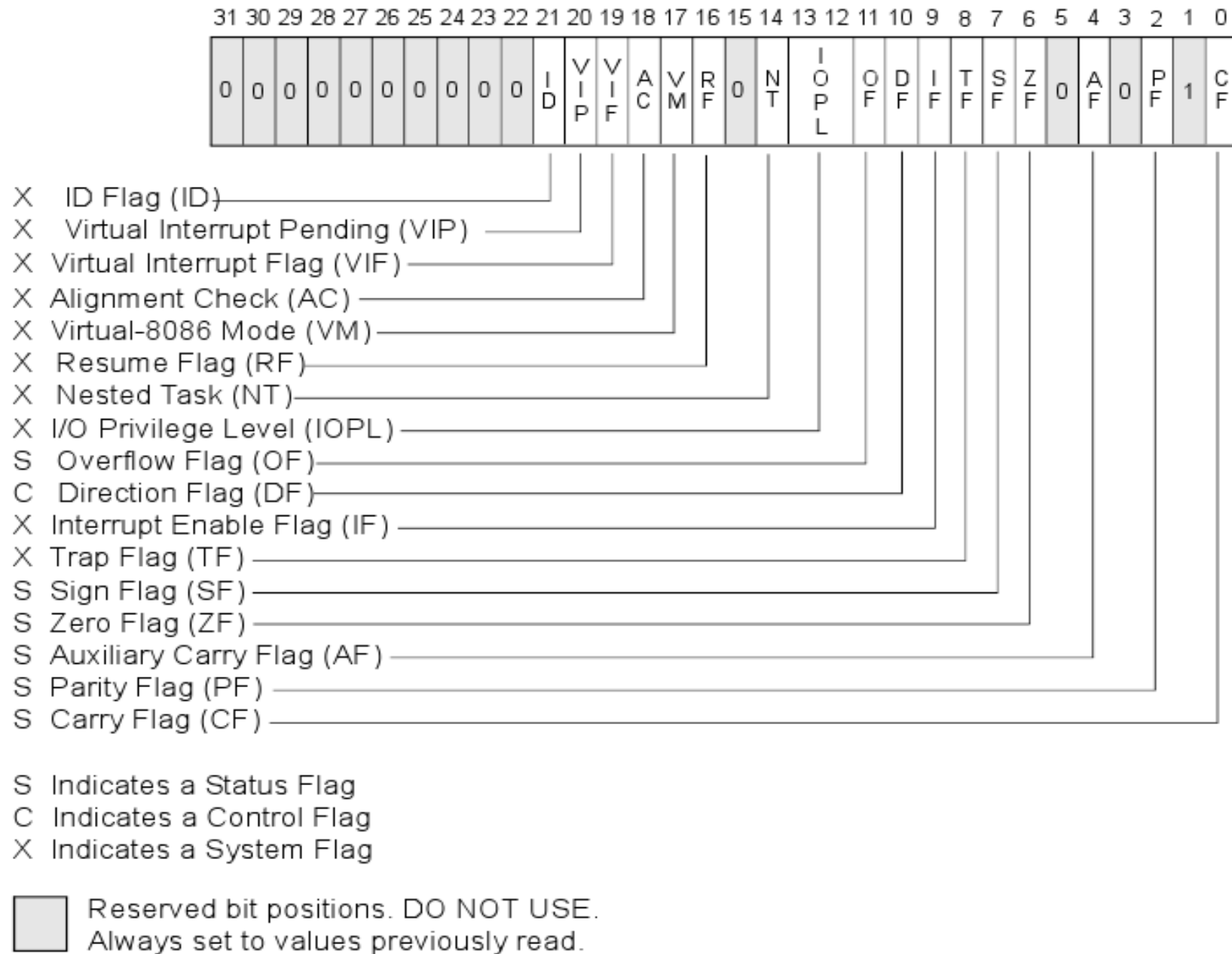


Figure 3-8. EFLAGS Register



EFLAGS

HLL:
IF'y, WHILE'e, FOR'y

Asm:
flagi + skoki warunkowe

EFLAGS

W wyniku ostatniej operacji
arytmetyczno-logicznej...

Flaga	Zgaszona Wyczyszczona (bit = 0) 	Zapalona Ustawiona (bit = 1) 
0 Carry Flag (CF)	Nie nastąpiło przeniesienie lub pożyczanie	Nastąpiło przeniesienie lub pożyczanie
2 Parity Flag (PF)	Liczba jedynek (zer) w wyniku była nieparzysta	Liczba jedynek (zer) w wyniku była parzysta
4 Aux Carry Flag (AF) (Adjust Flag)	Nie nastąpiło przeniesienie lub pożyczanie (4-bit BCD)	Nastąpiło przeniesienie lub pożyczanie (4-bit BCD)
6 Zero Flag (ZF)	Wynik był różny od zera	Wynikiem było zero
7 Sign Flag (SF)	W wyniku nie było minusa (tj. był dodatni)	W wyniku był minus (tj. był ujemny)
11 Overflow Flag (OF)	Nie nastąpiło przepełnienie	Nastąpiło przepełnienie

EFLAGS

**W wyniku ostatniej operacji
arytmetyczno-logicznej...**

**APPENDIX A - EFLAGS XREF
„Intel Manuals” Tom 1**

Let's play!

EFLAGS

Porównania...

CMP to SUB, ale...

$$X = A - B$$

- $X == 0$ -> A i B są równe**
- $X < 0$ -> A jest mniejsze**
- $X > 0$ -> A jest większe**
(flagi ?)

EFLAGS

Porównania...

TEST to AND, ale...

$$X = A \& B$$

(per bit: $1 \& 1 = 1$, pozostałe = 0)

Zazwyczaj:

TEST pole_bitowe, maska
(czy bit jest zapalony)

lub

TEST A,A

(czy A jest równe 0 ?)

EFLAGS

**Flagi, flagi, i co dalej?
Skoki warunkowe!**

**APPENDIX B - CC
„Intel Manuals” Tom 1**

**Jcc
„Intel Manuals” Tom 2a**

Let's play!

EFLAGS

Nie tylko skoki...

CMOVcc

„Intel Manuals” Tom 2a

SETcc

„Intel Manuals” Tom 2b

EFLAGS - Podsumowanie

**Gdy o 3ciej nad ranem obudzę Cię,
masz mi wyrecytować:**
(normalnie, na wspan i po rumuńsku)

- 1. Co to za flagi ZF, SF, OF i CF.**
- 2. Czym się różni SUB od CMP i
TEST od AND.**
- 3. Wymienić najczęściej stosowane
skoki warunkowe.**



Dziękuję za uwagę :)

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>