

Reverscraft

assembler

by gynvael.coldwind//vx

001 – Bliżej systemu...

Strony projektu:

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

Narzędzia:

FASM

<http://flatassembler.net/>

NASM

<http://www.nasm.us/>

GNU AS (Windows)

<http://mingw.org/>

GNU AS (*nix)

<http://gnu.org/software/binutils/>

**Poza tym: kalkulator, opcodes.txt
i manuale Intel'a**

Środowisko:

env.bat

```
set path=%path%;dysk:\katalog\fasm\  
set include=dysk:\katalog\fasm\include
```

fasmw.ini

```
[Environment]
```

```
Include=dysk:\katalog\fasm\include
```

Kod robiący nic:

Kod:

```
format PE GUI 4.0
```

```
mov eax, 0
```

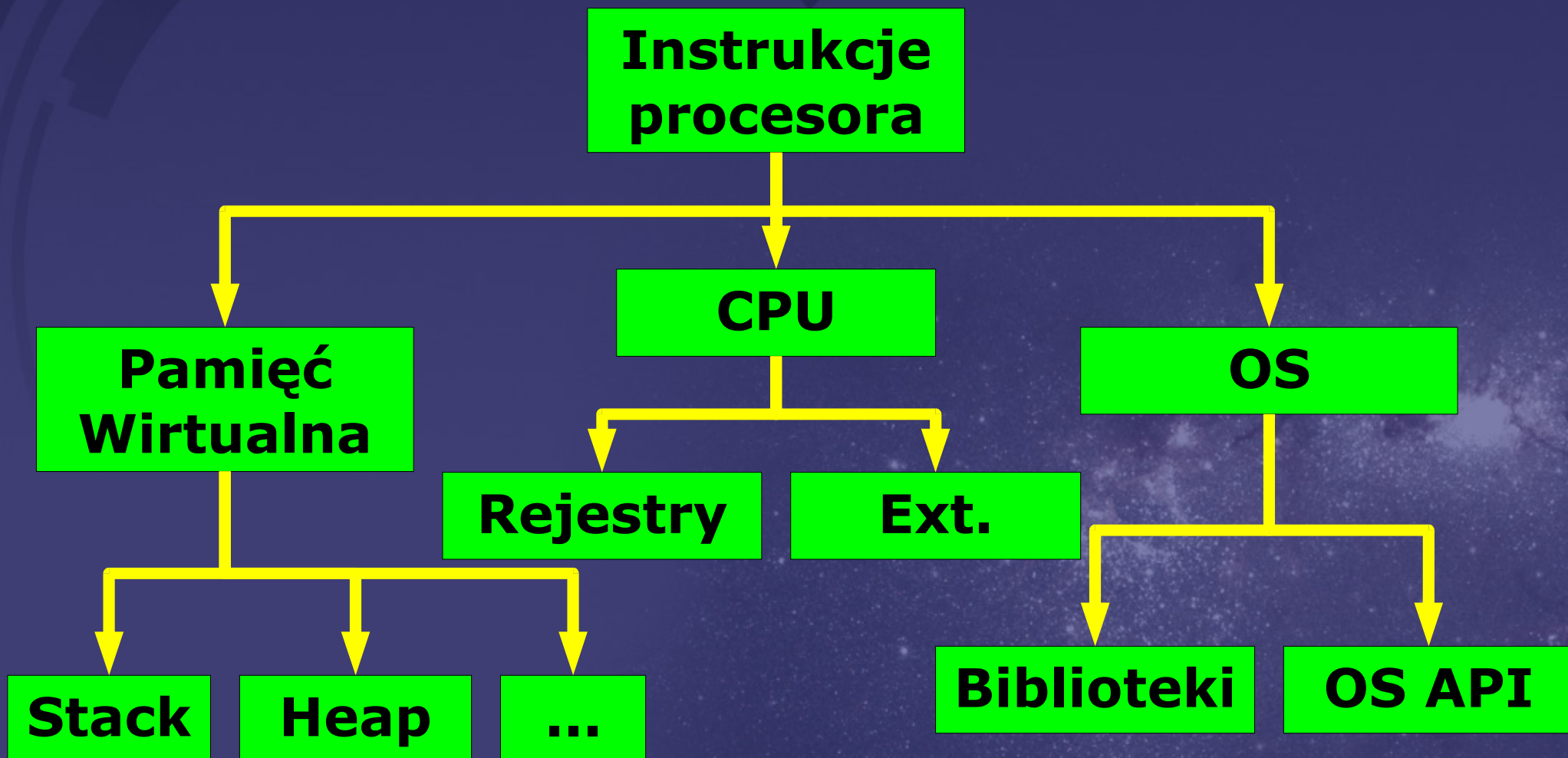
```
ret
```

Kompilacja:

```
fasm test1.asm
```

Zasoby!

czyli co możemy użyć...



Hello world!

```
include „win32a.inc“
```

```
data import
```

```
library user32, 'USER32.DLL'
```

```
import user32, \
```

```
    MessageBoxA, 'MessageBoxA'
```

```
end data
```

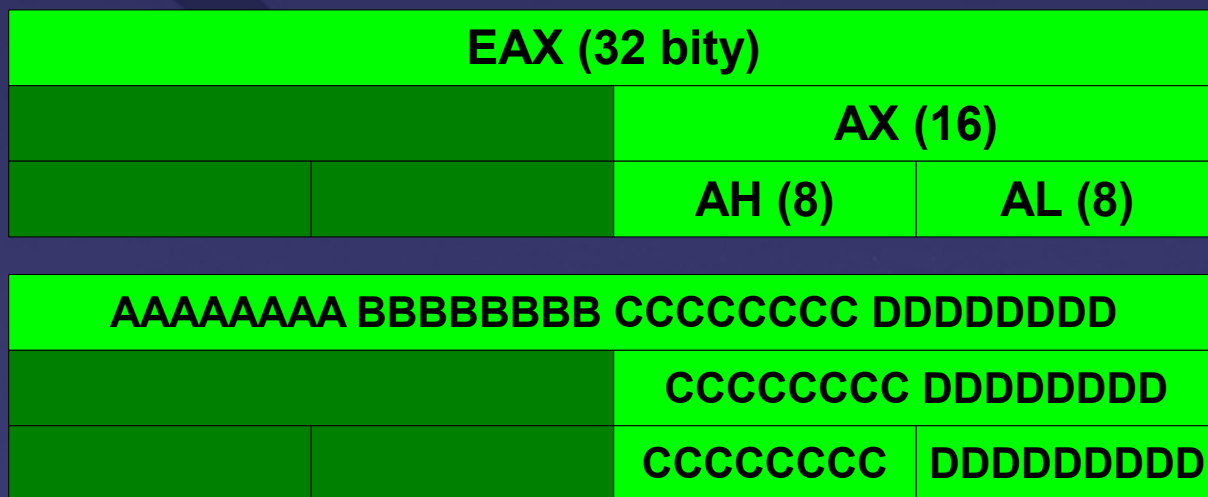
Podstawowe rejestry CPU:

eax → ax → ah, al
edx → dx → dh, dl
ecx → cx → ch, cl
ebx → bx → bh, bl

esi → si
edi → di

ebp → bp

esp → sp



eip
eflags

Przydatne biblioteki DLL:

msvcrt.dll

Microsoft C Runtime Library

kernel32.dll

WinAPI – pliki, procesy, etc

user32.dll

WinAPI - okna

gdi32.dll

WinAPI - rysowanie

opengl32.dll

glu32.dll

OpenGL API

wsock32.dll

ws2_32.dll

WinAPI - WinSOCK

„Kalkulator”!

1. Zapytać użytkownika o dwie liczby
2. Dodać je i wypisać wynik
3. Odjąć je i wypisać wynik
4. Pomnożyć je i wypisać wynik
5. Podzielić je i wypisać wynik
6. Zakończyć program



Dziękuję za uwagę :)

Strony projektu:

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