Basic Assembly

String representation

Assembly language programming
By xorpd

xorpd.net

Objectives

- We will learn how to represent text strings inside our assembly code.

Representing text

- How to express “Hello world” using ASCII?

48	65	6c	6c	6f	20	77	6f	72	6c	64

- We call this kind of representation a string of bytes, or just a **string**.

- How can we know the size of the string?

Schools of strings

- Two basic schools of indicating the size of a string:

- **Length prefix** (Pascal style):
  - Write the size of the string on the first byte.
  - 'Hello' is represented as:

05	48	65	6c	6c	6f

- **Null terminated** (C style):
  - The string ends (terminates) with the Null character (0).
  - 'Hello' is represented as:

48	65	6c	6c	6f	00

- There are some more representation systems. (Linked list, ropes etc.)

Schools of strings (Cont.)

	Length prefix	Null termination
Pros	• Length can be calculated quickly.	• The size of string is virtually unlimited.
Cons	• Size of string is limited. (If the length prefix is small).	• Takes longer time to calculate length. • Security issues: Strings can have no ending.

Schools of strings (Cont.)

- In this course we will work with **Null terminated strings.**
  - Windows API functions expect null terminated strings.
  - There are special assembly instructions to deal with null terminated objects.

Declaring strings

- The following declarations are equivalent:

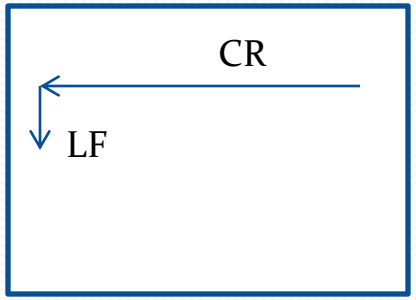
```
section '.data' data readable writeable
          ; Declare strings:

          str1    db  'Hello world',0

          str2    db  "Hello world",0

          str3    db  48h,65h,6ch,6ch,6fh,20h,77h,6fh,72h,6ch,64h,0

          str4    db  'Hell'
                  db  'o world',0

          str5    db  'Hello',20h,'world',0
```

New line

- Example:

- Different representations:
  - In Windows, a new line is marked by `0xd,0xa`.
  - In Linux, a new line is marked by `0xa`.

- Historic note:
  - CR (Carriage Return): `0xd`
    - Return to beginning of current line.
  - LF (Line Feed): `0xa`
    - Advance the paper one line forward.



Declaring strings with newline

- Example:

```
section '.data' data readable writeable
          ; Declare strings with more than one line:

          song    db  'Walking in the realms of brightness',13,10
                  db  'Passing the wall of above',0dh,0ah
                  db  'Down into the soul',0

          lines   db  'First line',0dh,0ah,'second line',0
```

Summary

- There are two basic ways to indicate the size of a string:
  - Length prefix (Pascal style)
  - Null termination (C style)
- Strings are declared using the **db** data syntax.
- New line is represented as:
  - `0xd,0xa` in windows.
  - `0xa` in linux

Exercise

- Assemble the given asm source file.
- Open the output using a hex editor.
- Identify the strings inside the output file.