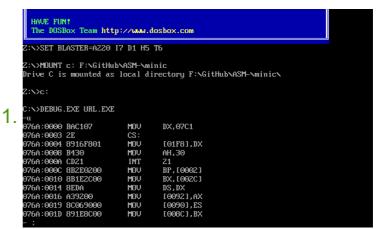
# 0531-研究试验2-宣讲会研究报告-尹

# 出忠恩

### H2 学习过程

- 1. 编写号url.c
  - 1. C url.c
- 2. 在 TC 中编译链接生成 url.exe
  - 1. III URLEXE
- 3. 用 DEBUG 调试 URL.EXE
  - 1. 按下 U 调试后不像是我所写的 url.c



2. 观察了一会儿,我试着看了看 076a:01f8 的出的 代码,看见下面几行是url.c 中所写的

```
-u 01f8
076A:01F8 0000
                          ADD
                                   [BX+SI],AL
076A:01FA 55
                          PUSH
                                  BP
076A:01FB 8BEC
                          MOV
                                  BP,SP
076A:01FD B80100
                          MOV
                                  AX,0001
                                  BX,0001
076A:0200 BB0100
                          MOV
076A:0203 B90200
                          MOV
                                  CX,000Z
076A:0206 8BC3
                          MOV
                                  AX,BX
076A:0208 03C1
                          ADD
                                  AX,CX
076a:020a 8ac7
                          MOV
                                  AL, BH
076A:020C 02C5
                                  AL,CH
                          ADD
076A:020E 8AE3
                          MOV
                                  AH,BL
                          ADD
076A:0210 02E1
                                  AH,CL
076A:0212 5D
                          POP
                                  ВP
076A:0213 C3
                          RET
076A:0214 C3
```

4. 修改url.c使其打印出main的地址(按十六进制)

重新编译运行后答应出main函数的地址

C:\>URL.EXE 1fa

- 5. 可以看到 1fa 处对应的代码为 push BP和 图 在第三步中观察到的一样
- 6. 编写,编译,链接,debug ur2.c, 跳转到main 函数执行位置可以看到在main函数中调用了子程序

	-U 1F8			
	076A:01F8	0000	ADD	[BX+SI],AL
	076A:01FA	55	PUSH	BP
	076A:01FB	8BEC	MOV	BP,SP
	076A:01FD	B80100	MOV	AX,0001
	076A:0200	BB0100	MOV	BX,0001
	076A:0203	B90200	MOV	CX,0002
	076A:0206	E80200	CALL	020B
1.	076A:0209	5D	POP	BP
	076A:020A	C3	RET	
	076A:020B	55	PUSH	BP
	076A:020C	8BEC	MOV	BP,SP
	076A:020E	8BC3	MOV	AX,BX
	076A:0210	0301	ADD	AX,CX
	076A:0212	5D	POP	BP
	076A:0213	C3	RET	
	076A:0214	C3	RET	

### H2 解决的问题

1. main函数在汇编语言的代码段中,

```
076A:0000 BAC107 MDV DX,07C1

076A:0003 ZE CS:

076A:0004 8916F801 MDV [01F8],DX

076A:0008 B430 MDV AH,30

076A:000A CD21 INT 21
```

- 2. 图中的 mov 01f8,dx 为main的人口地址
- 3. main函数应该也是一个代码段中的子功能

#### H2 研究体会

c 语言的函数调用本质上就是包装了汇编中的调用子函数和子程序返回的相关指令