Professor
Edson Pedro FERLIN

Segurança da Informação

Alteração Arquivo EXE

Prof. Edson Pedro Ferlin

Professor
Edson Pedro FERLIN

Segurança da Informação

Compiladores

Elemento-chave para a obtenção do desempenho

Fonte **Executável**

Exemplo de Compilação

PRINTF (“A”);

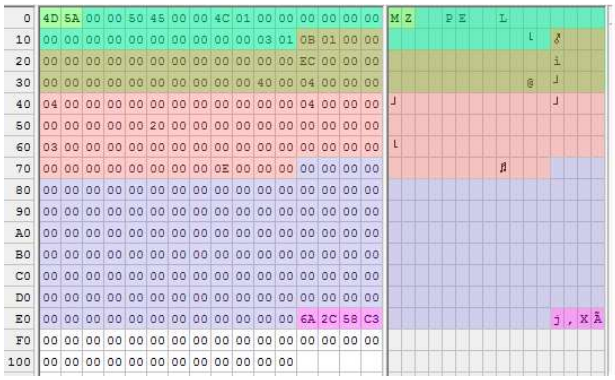
1011-1010-0100-0001-0000-0000
1011-0100-0000-0010
1100-1101-0010-0001

BA 41 00
B4 02
CD 21

MOV DX, #41h
MOV AH, #2h
INT 21h

Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	&#032;	Space	64	40	100	&#064;	@	96	60	140	&#096;	`
1	1	001	Start of Header	33	21	041	&#033;	!	65	41	101	&#065;	A	97	61	141	&#097;	a
2	2	002	Start of Text	34	22	042	&#034;	"	66	42	102	&#066;	B	98	62	142	&#098;	b
3	3	003	End of Text	35	23	043	&#035;	#	67	43	103	&#067;	C	99	63	143	&#099;	c
4	4	004	End of Transmission	36	24	044	&#036;	$	68	44	104	&#068;	D	100	64	144	&#100;	d
5	5	005	Enquiry	37	25	045	&#037;	%	69	45	105	&#069;	E	101	65	145	&#101;	e
6	6	006	Acknowledgment	38	26	046	&#038;	&	70	46	106	&#070;	F	102	66	146	&#102;	f
7	7	007	Bell	39	27	047	&#039;	'	71	47	107	&#071;	G	103	67	147	&#103;	g
8	8	010	Backspace	40	28	050	&#040;	(	72	48	110	&#072;	H	104	68	150	&#104;	h
9	9	011	Horizontal Tab	41	29	051	&#041;	)	73	49	111	&#073;	I	105	69	151	&#105;	i
10	A	012	Line feed	42	2A	052	&#042;	*	74	4A	112	&#074;	J	106	6A	152	&#106;	j
11	B	013	Vertical Tab	43	2B	053	&#043;	+	75	4B	113	&#075;	K	107	6B	153	&#107;	k
12	C	014	Form feed	44	2C	054	&#044;	,	76	4C	114	&#076;	L	108	6C	154	&#108;	l
13	D	015	Carriage return	45	2D	055	&#045;	-	77	4D	115	&#077;	M	109	6D	155	&#109;	m
14	E	016	Shift Out	46	2E	056	&#046;	.	78	4E	116	&#078;	N	110	6E	156	&#110;	n
15	F	017	Shift In	47	2F	057	&#047;	/	79	4F	117	&#079;	O	111	6F	157	&#111;	o
16	10	020	Data Link Escape	48	30	060	&#048;	0	80	50	120	&#080;	P	112	70	160	&#112;	p
17	11	021	Device Control 1	49	31	061	&#049;	1	81	51	121	&#081;	Q	113	71	161	&#113;	q
18	12	022	Device Control 2	50	32	062	&#050;	2	82	52	122	&#082;	R	114	72	162	&#114;	r
19	13	023	Device Control 3	51	33	063	&#051;	3	83	53	123	&#083;	S	115	73	163	&#115;	s
20	14	024	Device Control 4	52	34	064	&#052;	4	84	54	124	&#084;	T	116	74	164	&#116;	t
21	15	025	Negative Ack.	53	35	065	&#053;	5	85	55	125	&#085;	U	117	75	165	&#117;	u
22	16	026	Synchronous idle	54	36	066	&#054;	6	86	56	126	&#086;	V	118	76	166	&#118;	v
23	17	027	End of Trans. Block	55	37	067	&#055;	7	87	57	127	&#087;	W	119	77	167	&#119;	w
24	18	030	Cancel	56	38	070	&#056;	8	88	58	130	&#088;	X	120	78	170	&#120;	x
25	19	031	End of Medium	57	39	071	&#057;	9	89	59	131	&#089;	Y	121	79	171	&#121;	y
26	1A	032	Substitute	58	3A	072	&#058;	:	90	5A	132	&#090;	Z	122	7A	172	&#122;	z
27	1B	033	Escape	59	3B	073	&#059;	;	91	5B	133	&#091;	[	123	7B	173	&#123;	{
28	1C	034	File Separator	60	3C	074	&#060;	<	92	5C	134	&#092;	\	124	7C	174	&#124;	|
29	1D	035	Group Separator	61	3D	075	&#061;	=	93	5D	135	&#093;	]	125	7D	175	&#125;	}
30	1E	036	Record Separator	62	3E	076	&#062;	>	94	5E	136	&#094;	^	126	7E	176	&#126;	~
31	1F	037	Unit Separator	63	3F	077	&#063;	?	95	5F	137	&#095;	_	127	7F	177	&#127;	Del

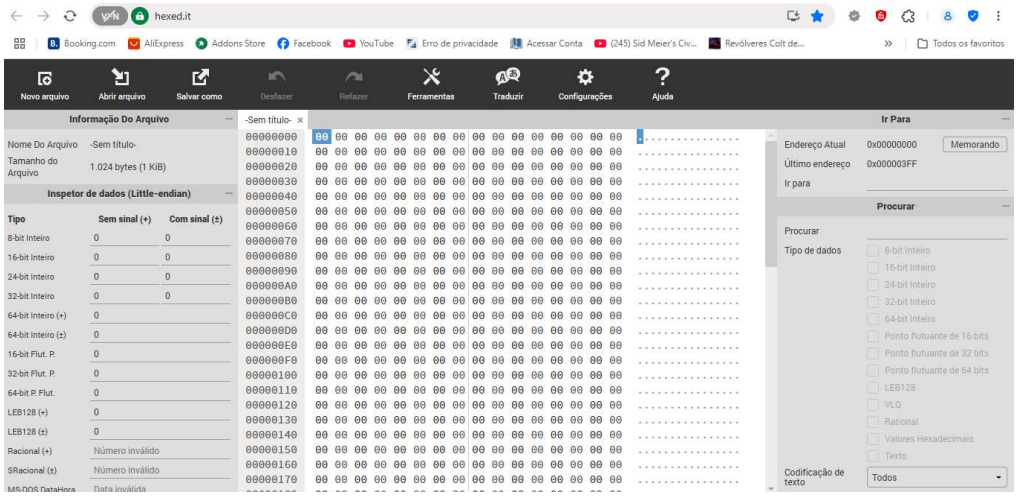
Estrutura – Arquivo EXE




```
0x6A // PUSH
0x2C // value to push
0x58 // POP EAX
0xC3 // RETN
```

268 bytes is the absolute minimum size for a working executable under Windows 7 64-bit edition

Site HEXED.IT



Arquivo TESTE.EXE

-Sem título- × Teste.exe ×

```
000025B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000025C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000025D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000025E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000025F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00002600  4F 6C 61 21 20 54 75 72 6D 61 20 76 61 6D 6F 73  Ola! Turma vamos
00002610  20 63 6F 6D 65 63 61 72 21 20 00 00 00 00 00 00   comecar! ......
00002620  41 72 67 75 6D 65 6E 74 20 64 6F 6D 61 69 6E 20  Argument domain
00002630  65 72 72 6F 72 20 28 44 4F 4D 41 49 4E 29 00 41  error (DOMAIN).A
00002640  72 67 75 6D 65 6E 74 20 73 69 6E 67 75 6C 61 72  rgument singular
00002650  69 74 79 20 28 53 49 47 4E 29 00 00 00 00 00 00  ity (SIGN)......
00002660  4F 76 65 72 66 6C 6F 77 20 72 61 6E 67 65 20 65  Overflow range e
00002670  72 72 6F 72 20 28 4F 56 45 52 46 4C 4F 57 29 00  rror (OVERFLOW).
00002680  50 61 72 74 69 61 6C 20 6C 6F 73 73 20 6F 66 20  Partial loss of
00002690  73 69 67 6E 69 66 69 63 61 6E 63 65 20 28 50 4C  significance (PL
000026A0  4F 53 53 29 00 00 00 00 54 6F 74 61 6C 20 6C 6F  OSS)....Total lo
000026B0  73 73 20 6F 66 20 73 69 67 6E 69 66 69 63 61 6E  ss of significan
000026C0  63 65 20 28 54 4C 4F 53 53 29 00 00 00 00 00 00  ce (TLOSS)......
```


Professor
Edson Pedro FERLIN

Segurança da Informação

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) ProfEdsonPedroFerlin