

Alteração Arquivo EXE

Prof. Edson Pedro Ferlin

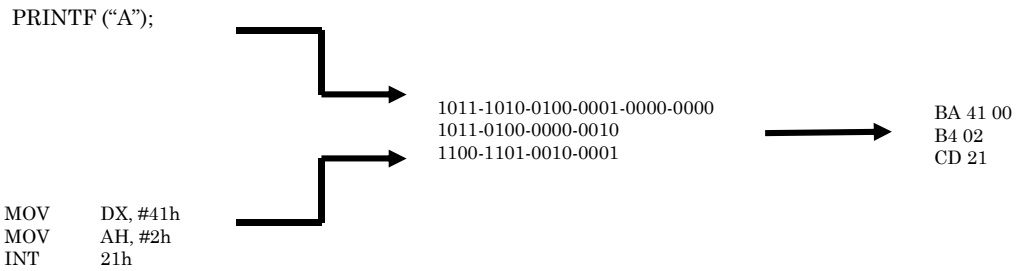
Compiladores

Elemento-chave para a obtenção do desempenho

Fonte  Executável



Exemplo de Compilação



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

Estrutura – Arquivo EXE

0	4D 5A 00 00 50 45 00 00 4C 01 00 00 00 00 00 00	M Z P E L
10	00 00 00 00 00 00 00 00 00 00 03 01 0B 01 00 00	L
20	00 00 00 00 00 00 00 00 00 00 00 00 EC 00 00 00	I
30	00 00 00 00 00 00 00 00 00 00 40 00 04 00 00 00	S J
40	04 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00	J
50	00 00 00 00 00 20 00 00 00 00 00 00 00 00 00 00	L
60	03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	#
70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
100	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

- DOS Header
- PE Header overlaps DOS
- Optional Header overlaps DOS
- Optional Header
- Data Directories
- Program Code

```
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

The screenshot shows the HEXED.IT website interface. At the top, there are navigation buttons: 'Novo arquivo', 'Abrir arquivo', 'Salvar como', 'Desfazer', 'Refazer', 'Ferramentas', 'Traduzir', 'Configurações', and 'Ajuda'. Below this, the 'Informação Do Arquivo' section displays file details: 'Nome Do Arquivo: -Sem título-', 'Tamanho do Arquivo: 1.024 bytes (1 KiB)', and 'Inspeção de dados (Little-endian)'. The main area is a hex editor showing a grid of hex values (mostly 00) and their corresponding ASCII characters. On the right side, there is a 'Procurar' (Search) section with options for 'Tipo de dados' (Data type) such as 8-bit, 16-bit, 24-bit, 32-bit, and 64-bit integers, and a 'Codificação de texto' (Text encoding) dropdown menu.

Arquivo TESTE.EXE

-Sem título- x	Teste.exe x	
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).....

Contato



eferlin@live.com



(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) [ProfEdsonPedroFerlin](https://www.youtube.com/ProfEdsonPedroFerlin)