x86 Short Jump Cheat Sheet

by @VelloSec / vellosec.net

HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES
01	1	10	16	1f	31	2e	46	3d	61	4c	76	5b	91	6a	106	79	121
02	2	11	17	20	32	2f	47	3e	62	4d	77	5c	92	6b	107	7a	122
03	3	12	18	21	33	30	48	3f	63	4e	78	5d	93	6c	108	7b	123
04	4	13	19	22	34	31	49	40	64	4f	79	5e	94	6d	109	7c	124
05	5	14	20	23	35	32	50	41	65	50	80	5f	95	6e	110	7d	125
06	6	15	21	24	36	33	51	42	66	51	81	60	96	6f	111	7e	126
07	7	16	22	25	37	34	52	43	67	52	82	61	97	70	112	7f	127
08	8	17	23	26	38	35	53	44	68	53	83	62	98	71	113		
09	9	18	24	27	39	36	54	45	69	54	84	63	99	72	114		
0a	10	19	25	28	40	37	55	46	70	55	85	64	100	73	115		
0b	11	1a	26	29	41	38	56	47	71	56	86	65	101	74	116		
0c	12	1b	27	2a	42	39	57	48	72	57	87	66	102	75	117		
0d	13	1c	28	2b	43	3a	58	49	73	58	88	67	103	76	118		
0e	14	1d	29	2c	44	3b	59	4a	74	59	89	68	104	77	119		
0f	15	1e	30	2d	45	3c	60	4b	75	5a	90	69	105	78	120		

HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES	HEX	BYTES
80	-128	8f	-113	9e	-98	ad	-83	bc	-68	cb	-53	da	-38	e9	-23	f8	-8
81	-127	90	-112	9f	-97	ae	-82	bd	-67	cc	-52	db	-37	ea	-22	f9	-7
82	-126	91	-111	a0	-96	af	-81	be	-66	cd	-51	dc	-36	eb	-21	fa	-6
83	-125	92	-110	a1	-95	b0	-80	bf	-65	ce	-50	dd	-35	ec	-20	fb	-5
84	-124	93	-109	a2	-94	b1	-79	c0	-64	cf	-49	de	-34	ed	-19	fc	-4
85	-123	94	-108	a3	-93	b2	-78	c1	-63	d0	-48	df	-33	ee	-18	fd	-3
86	-122	95	-107	a4	-92	b3	-77	c2	-62	d1	-47	e0	-32	ef	-17	fe	-2
87	-121	96	-106	a5	-91	b4	-76	c3	-61	d2	-46	e1	-31	f0	-16	ff	-1
88	-120	97	-105	a6	-90	b5	-75	c4	-60	d3	-45	e2	-30	f1	-15		
89	-119	98	-104	a7	-89	b6	-74	c5	-59	d4	-44	e3	-29	f2	-14		
8a	-118	99	-103	a8	-88	b7	-73	c6	-58	d5	-43	e4	-28	f3	-13		
8b	-117	9a	-102	a9	-87	b8	-72	c7	-57	d6	-42	e5	-27	f4	-12		
8c	-116	9b	-101	aa	-86	b9	-71	c8	-56	d7	-41	e6	-26	f5	-11		
8d	-115	9c	-100	ab	-85	ba	-70	c9	-55	d8	-40	e7	-25	f6	-10		
8e	-114	9d	-99	ac	-84	bb	-69	ca	-54	d9	-39	e8	-24	f7	-9		

HEX	Represents the HEX value that will be used for your short jump
BYTES	Represents the number of bytes to jump. Remember, the jump begins after the two bytes used in the jump. This means that you lose two bytes when jumping backwards.