

Sheet1

0xbfffeb60		0xbfffeb97	dir de str (arg bof)
0xbfffeb5c = (buffer + 36)		0x8048574	r.a. de bof
0xbfffeb58	ebp →	ebp main	
		.	
		.	
0xbfffeb50		buffer[23]	
0xbfffeb4f		buffer[22]	
		.	
		.	
0xbfffeb38 = (ebp - 32)		buffer[0]	
		.	
		.	
0xbfffeb24		0xbfffeb97	dir de str (arg 2 strcpy)
0xbfffeb38	esp →	0xbfffeb38	dir de buffer (arg 1 strcpy)