

```
0 : 08048300 [ 2] xor %ebp, %ebp
1 : 08048302 [ 1] pop %esi
2 : 08048303 [ 2] mov %esp, %ecx
3 : 08048305 [ 3] and $0xF0, %esp
4 : 08048308 [ 1] push %eax
5 : 08048309 [ 1] push %esp
6 : 0804830a [ 1] push %edx
7 : 0804830b [ 5] push $0x08048430
8 : 08048310 [ 5] push $0x08048440
9 : 08048315 [ 1] push %ecx
10 : 08048316 [ 1] push %esi
11 : 08048317 [ 5] push $0x080483D7
12 : 0804831c [ 5] lcall 0x080482E8
13 : 08048321 [ 1] hlt
14 : 08048322 [ 1] nop
15 : 08048323 [ 1] nop
16 : 08048324 [ 1] nop
17 : 08048325 [ 1] nop
18 : 08048326 [ 1] nop
19 : 08048327 [ 1] nop
20 : 08048328 [ 1] nop
21 : 08048329 [ 1] nop
22 : 0804832a [ 1] nop
23 : 0804832b [ 1] nop
24 : 0804832c [ 1] nop
25 : 0804832d [ 1] nop
26 : 0804832e [ 1] nop
27 : 0804832f [ 1] nop
28 : 08048330 [ 1] push %ebp
29 : 08048331 [ 2] mov %esp, %ebp
30 : 08048333 [ 1] push %ebx
31 : 08048334 [ 3] sub $0x04, %esp
32 : 08048337 [ 7] cmpb $0x00, 0x804A010
33 : 0804833e [ 2] jnz 0x0804837F
```

```
34 : 08048340 [ 5] movl 0x0804A014, %eax
35 : 08048345 [ 5] mov $0x08049F18, %ebx
36 : 0804834a [ 6] sub $0x08049F14, %ebx
37 : 08048350 [ 3] sar $0x02, %ebx
38 : 08048353 [ 3] sub $0x01, %ebx
39 : 08048356 [ 2] cmp %ebx, %eax
40 : 08048358 [ 2] jnc 0x08048378
```

```
41 : 0804835a [ 6] leal (%esi), %esi
```

```
42 : 08048360 [ 3] add $0x01, %eax
43 : 08048363 [ 5] movl %eax, 0x0804A014
44 : 08048368 [ 7] lcall *0x8049F14(, %eax, 4)
45 : 0804836f [ 5] movl 0x0804A014, %eax
46 : 08048374 [ 2] cmp %ebx, %eax
47 : 08048376 [ 2] jc 0x08048360
```

```
48 : 08048378 [ 7] movb $0x01, 0x804A010
```

```
49 : 0804837f [ 3] add $0x04, %esp
50 : 08048382 [ 1] pop %ebx
51 : 08048383 [ 1] pop %ebp
52 : 08048384 [ 1] ret
```

```
53 : 08048385 [ 4] leal (%esi), %esi
54 : 08048389 [ 7] leal (%edi), %edi
55 : 08048390 [ 1] push %ebp
56 : 08048391 [ 2] mov %esp, %ebp
57 : 08048393 [ 3] sub $0x18, %esp
58 : 08048396 [ 5] movl 0x08049F1C, %eax
59 : 0804839b [ 2] test %eax, %eax
60 : 0804839d [ 1] jz 0x080483B1
```

```
61 : 0804839f [ 5] mov $0x00000000, %eax
62 : 080483a4 [ 2] test %eax, %eax
63 : 080483a6 [ 2] jz 0x080483B1
```

```
64 : 080483a8 [ 7] movl $0x08049F1C, (%esp)
65 : 080483af [ 2] lcall %eax
```

```
66 : 080483b1 [ 1] leave
67 : 080483b2 [ 1] ret
```

```
68 : 080483b3 [ 1] nop
69 : 080483b4 [ 1] push %ebp
70 : 080483b5 [ 2] mov %esp, %ebp
71 : 080483b7 [ 3] sub $0x10, %esp
72 : 080483ba [ 7] movl $0x0000DEAD, -0x4(%ebp)
73 : 080483c1 [ 3] movl 0x8(%ebp), %edx
74 : 080483c4 [ 2] mov %edx, %eax
75 : 080483c6 [ 2] add %eax, %eax
76 : 080483c8 [ 2] add %edx, %eax
77 : 080483ca [ 5] add $0x0000BEEF, %eax
78 : 080483cf [ 3] addl %eax, -0x4(%ebp)
79 : 080483d2 [ 3] movl -0x4(%ebp), %eax
80 : 080483d5 [ 1] leave
81 : 080483d6 [ 1] ret
```

```
82 : 080483d7 [ 1] push %ebp
83 : 080483d8 [ 2] mov %esp, %ebp
84 : 080483da [ 1] push %ebx
85 : 080483db [ 3] sub $0x34, %esp
86 : 080483de [ 7] movl $0x00000000, -0x8(%ebp)
87 : 080483e5 [ 2] ljmp 0x08048413
```

```
100 : 08048413 [ 4] cmpl $0x09, -0x8(%ebp)
101 : 08048417 [ 2] jle 0x080483E7
```

```
88 : 080483e7 [ 3] movl -0x8(%ebp), %ebx
89 : 080483ea [ 3] movl -0x8(%ebp), %eax
90 : 080483ed [ 3] movl %eax, (%esp)
91 : 080483f0 [ 5] lcall 0x080483B4
92 : 080483f5 [ 4] movl %eax, -0x30(%ebp, %ebx, 4)
93 : 080483f9 [ 3] movl -0x8(%ebp), %eax
94 : 080483fc [ 4] movl -0x30(%ebp, %eax, 4), %eax
95 : 08048400 [ 2] test %eax, %eax
96 : 08048402 [ 2] jnz 0x0804840F
```

```
102 : 08048419 [ 5] mov $0x00000000, %eax
103 : 0804841e [ 3] add $0x34, %esp
104 : 08048421 [ 1] pop %ebx
105 : 08048422 [ 1] pop %ebp
106 : 08048423 [ 1] ret
```

```
97 : 08048404 [ 3] movl -0x8(%ebp), %eax
98 : 08048407 [ 8] movl $0xBAADF00D, -0x30(%ebp, %eax, 4)
```

```
99 : 0804840f [ 4] addl $0x01, -0x8(%ebp)
```

```
107 : 08048424 [ 1] nop
108 : 08048425 [ 1] nop
109 : 08048426 [ 1] nop
110 : 08048427 [ 1] nop
111 : 08048428 [ 1] nop
112 : 08048429 [ 1] nop
113 : 0804842a [ 1] nop
114 : 0804842b [ 1] nop
115 : 0804842c [ 1] nop
116 : 0804842d [ 1] nop
117 : 0804842e [ 1] nop
118 : 0804842f [ 1] nop
119 : 08048430 [ 1] push %ebp
120 : 08048431 [ 2] mov %esp, %ebp
121 : 08048433 [ 1] pop %ebp
122 : 08048434 [ 1] ret
```

```
123 : 08048435 [ 4] leal (%esi), %esi
124 : 08048439 [ 7] leal (%edi), %edi
125 : 08048440 [ 1] push %ebp
126 : 08048441 [ 2] mov %esp, %ebp
127 : 08048443 [ 1] push %edi
128 : 08048444 [ 1] push %esi
129 : 08048445 [ 1] push %ebx
130 : 08048446 [ 5] lcall 0x0804849A
131 : 0804844b [ 6] add $0x00001BA9, %ebx
132 : 08048451 [ 3] sub $0x1C, %esp
133 : 08048454 [ 5] lcall 0x08048298
134 : 08048459 [ 6] leal -0xE8(%ebx), %edi
135 : 0804845f [ 6] leal -0xE8(%ebx), %eax
136 : 08048465 [ 2] sub %eax, %edi
137 : 08048467 [ 3] sar $0x02, %edi
138 : 0804846a [ 2] test %edi, %edi
139 : 0804846c [ 2] jz 0x08048492
```

```
140 : 0804846e [ 2] xor %esi, %esi
```

```
141 : 08048470 [ 3] movl 0x10(%ebp), %eax
142 : 08048473 [ 4] movl %eax, 0x8(%esp)
143 : 08048477 [ 3] movl 0xC(%ebp), %eax
144 : 0804847a [ 4] movl %eax, 0x4(%esp)
145 : 0804847e [ 3] movl 0x8(%ebp), %eax
146 : 08048481 [ 3] movl %eax, (%esp)
147 : 08048484 [ 7] lcall *-0xE8(%ebx, %esi, 4)
148 : 0804848b [ 3] add $0x01, %esi
149 : 0804848e [ 2] cmp %edi, %esi
150 : 08048490 [ 2] jc 0x08048470
```

```
151 : 08048492 [ 3] add $0x1C, %esp
152 : 08048495 [ 1] pop %ebx
153 : 08048496 [ 1] pop %esi
154 : 08048497 [ 1] pop %edi
155 : 08048498 [ 1] pop %ebp
156 : 08048499 [ 1] ret
```

```
157 : 0804849a [ 3] movl (%esp), %ebx
158 : 0804849d [ 1] ret
```

```
159 : 0804849e [ 1] nop
160 : 0804849f [ 1] nop
161 : 080484a0 [ 1] push %ebp
162 : 080484a1 [ 2] mov %esp, %ebp
163 : 080484a3 [ 1] push %ebx
164 : 080484a4 [ 3] sub $0x04, %esp
165 : 080484a7 [ 5] movl 0x08049F0C, %eax
166 : 080484ac [ 3] cmp $0xFF, %eax
167 : 080484af [ 2] jz 0x080484C4
```

```
168 : 080484b1 [ 5] mov $0x08049F0C, %ebx
169 : 080484b6 [ 2] nop
```

```
170 : 080484b8 [ 3] sub $0x04, %ebx
171 : 080484bb [ 2] lcall %eax
172 : 080484bd [ 2] movl (%ebx), %eax
173 : 080484bf [ 3] cmp $0xFF, %eax
174 : 080484c2 [ 2] jnz 0x080484B8
```

```
175 : 080484c4 [ 3] add $0x04, %esp
176 : 080484c7 [ 1] pop %ebx
177 : 080484c8 [ 1] pop %ebp
178 : 080484c9 [ 1] ret
```

```
179 : 080484ca [ 1] nop
180 : 080484cb [ 1] nop
```