

1/8

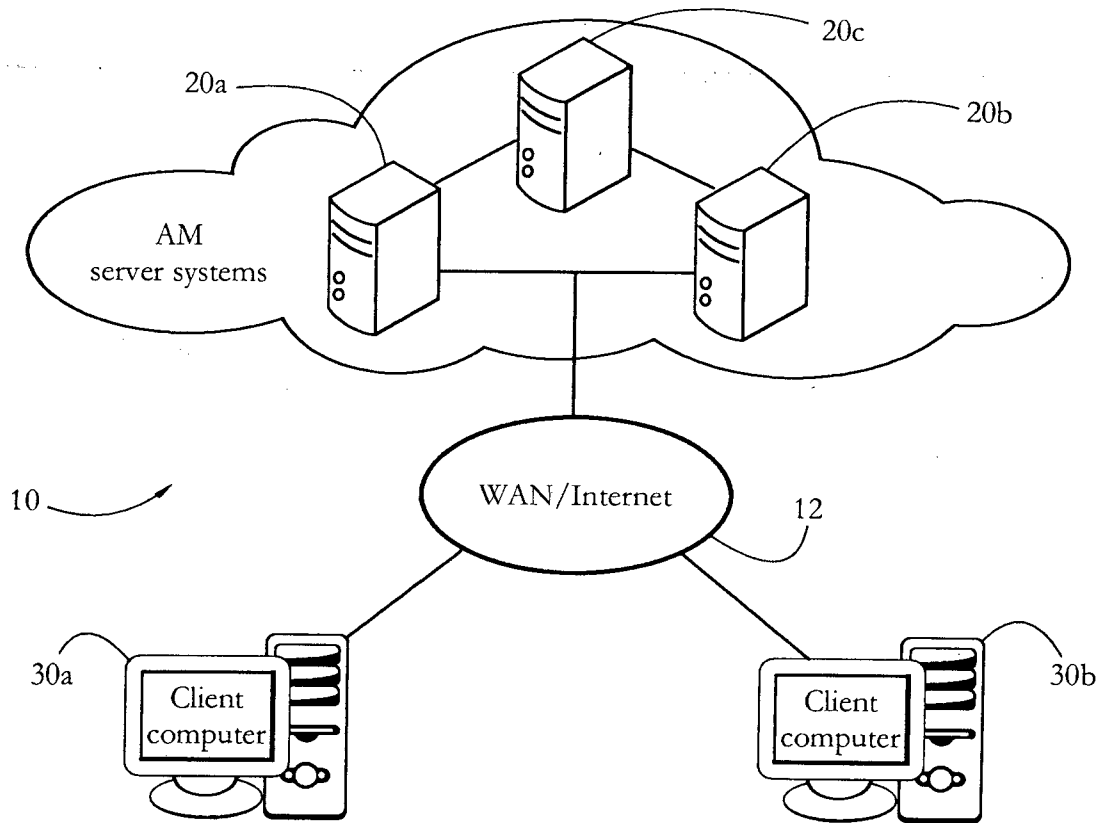


FIG. 1

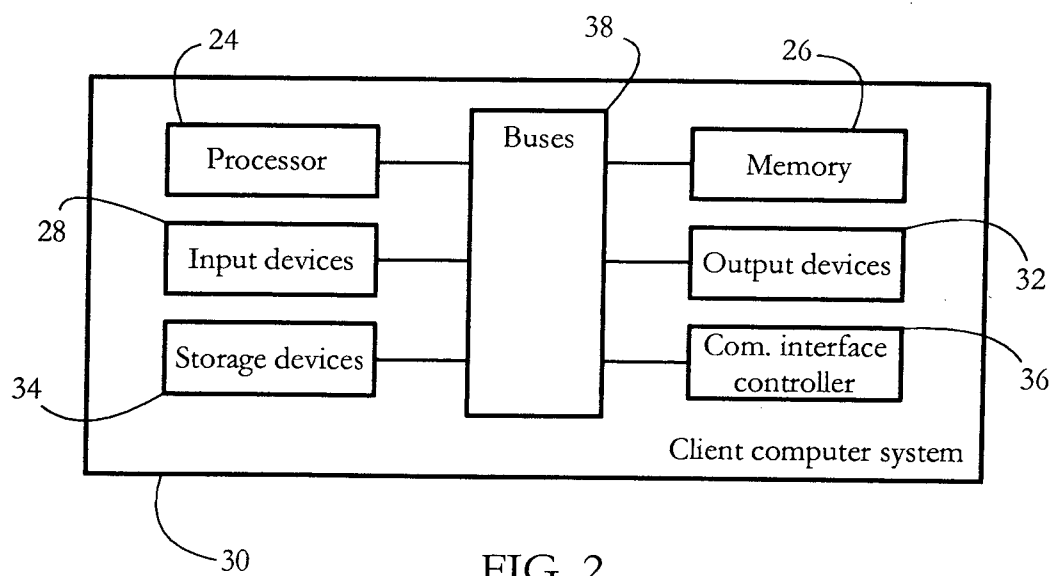


FIG. 2

2/8

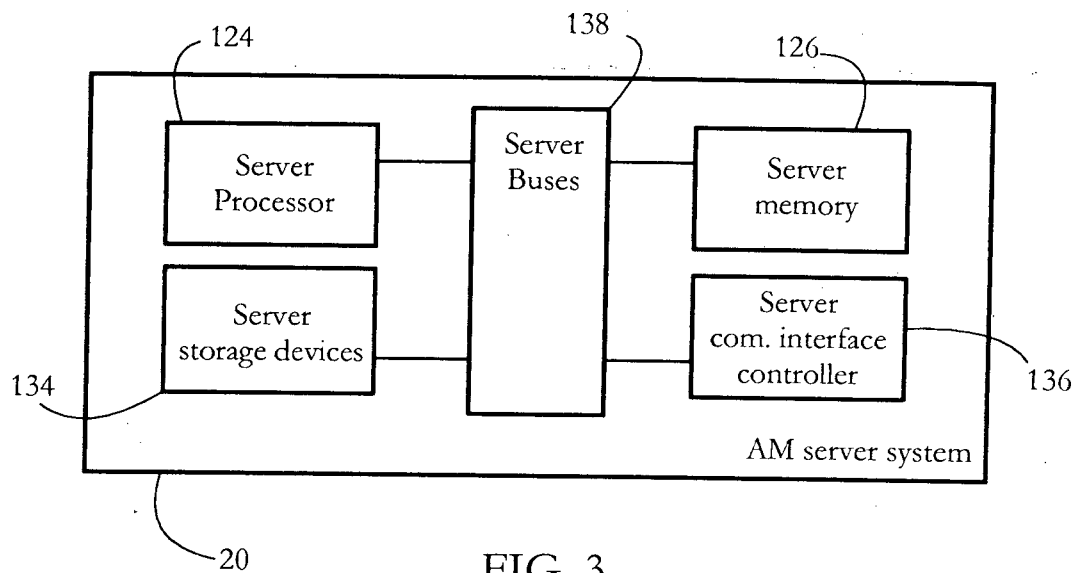


FIG. 3

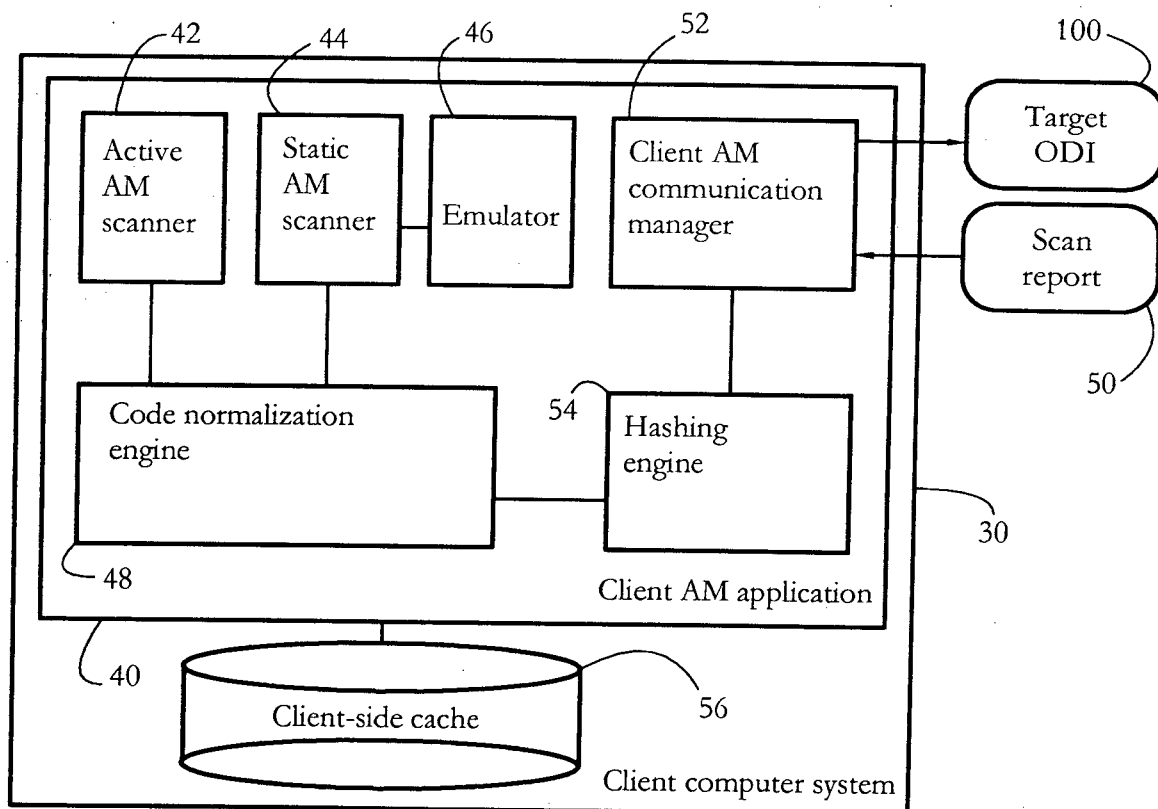


FIG. 4

3/8

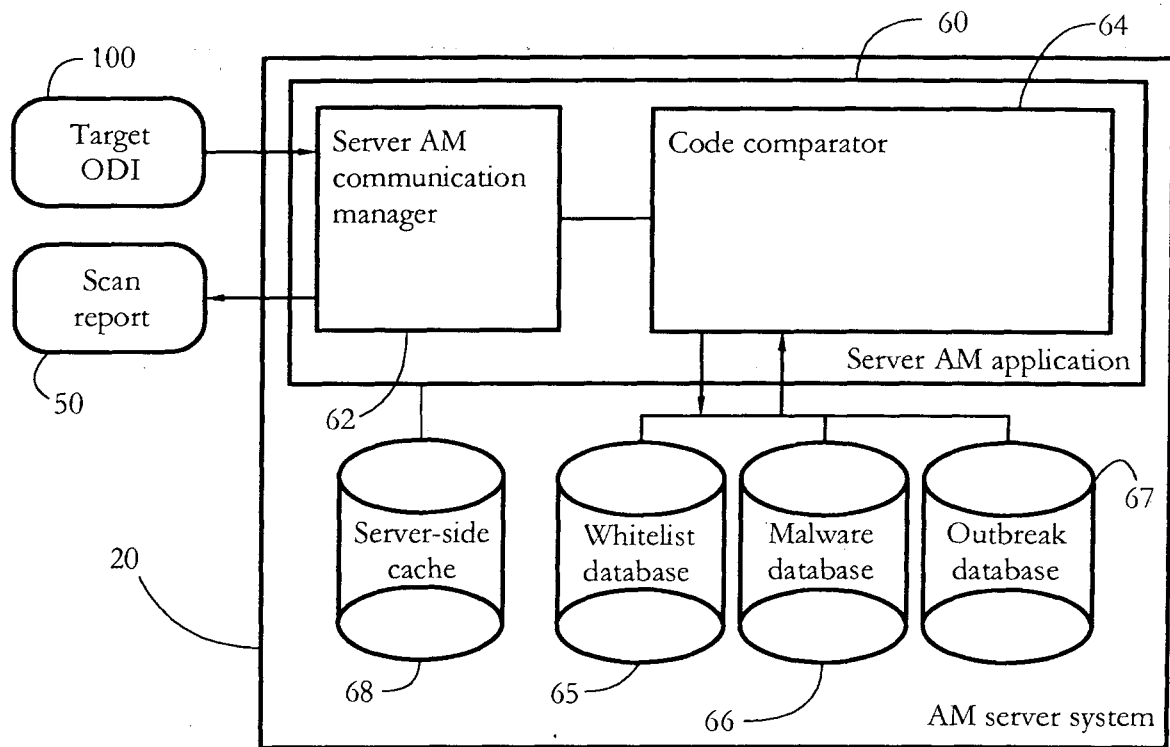
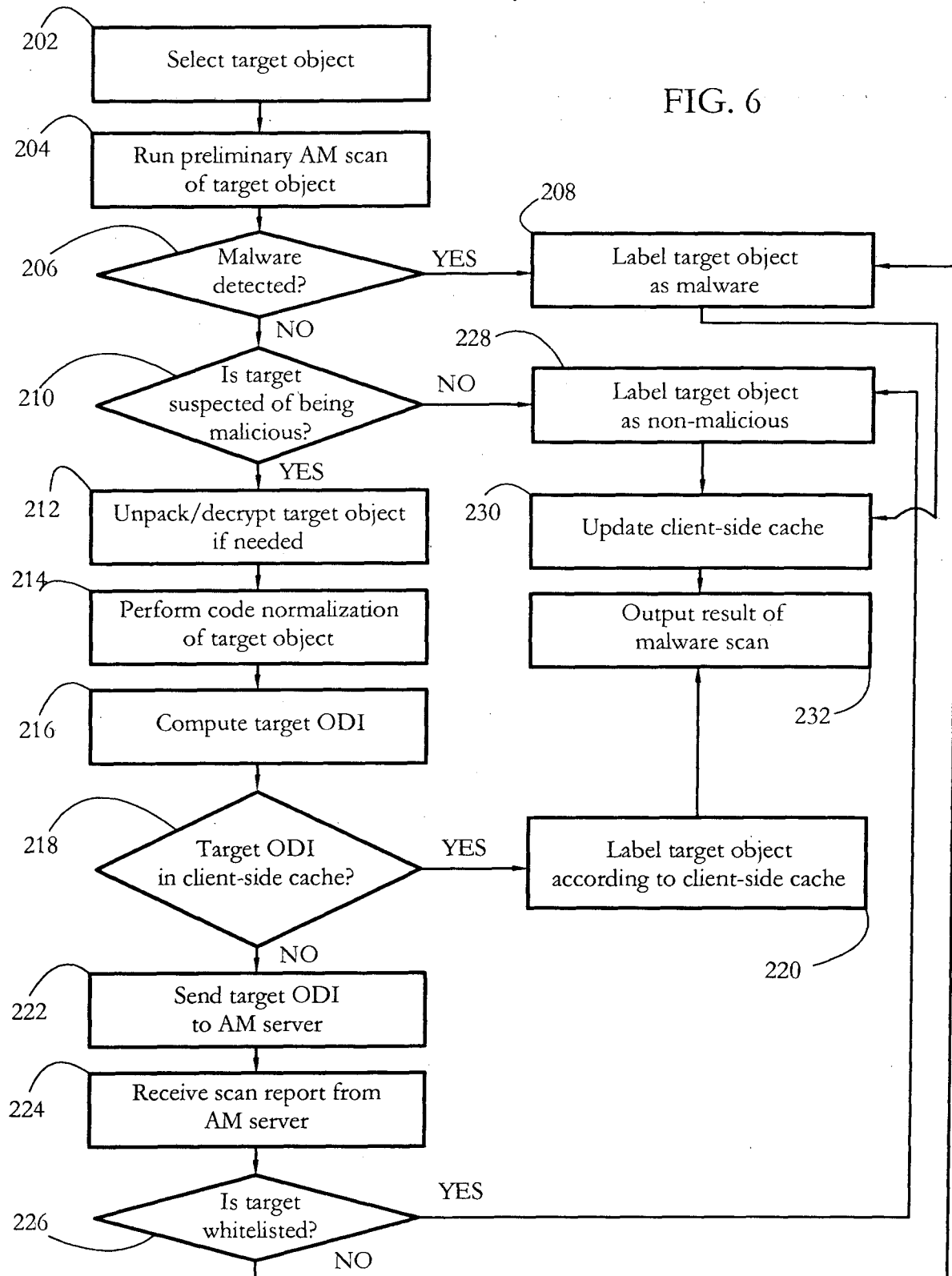


FIG. 5

4/8

FIG. 6



5/8

```
PUSH EBP
MOV EBP, ESP
```

```
PUSH EAX
XOR EAX, EAX
MOV EAX, 0x4
ADD EAX, 0x7
SUB EAX, 0x0
CMP EAX, 0x10
JE 0x405600
PUSH 0x2
POP EBX
```

```
SUB EAX, EBX
CALL 0x401000
JMP 0x401200
PUSH EDX
MOV EDX, 2
XOR EDX, EAX
TEST EAX, EAX
JNZ 0x402006
LEA ECX, [ECX + 0x0]
PUSH ECX
PUSH EAX
CALL 0x401000
MOV ESP, EBP
POP EBP
```

```
; EBP will be replaced with EAX
; ESP will be replaced with ECX
; end of function prolog -> will be removed
; EAX will be replaced with EDX
; sets EAX to 0 -> will be removed
; MOV operation -> removed
; replaced with ADD EDX, 0x0
; does not modify EAX -> removed
; CMP operation -> removed
; replaced with JE 0x0
; PUSH followed by POP -> replaced with MOV EBX,
; 0x0, and therefore removed
; replaced with SUB EDX, EBX
; replaced with CALL 0x0
; replaced with JMP 0x0
; EDX will be replaced with ESP
; MOV operation -> removed
; replaced with XOR ESP, EDX
; TEST operation -> removed
; replaced with JNE 0x0
; replaced with MOV EBP, 0 and removed
; replaced with PUSH EBP
; replaced with PUSH EDX
; replaced with CALL 0x0
; end of function epilog -> removed
```



70

```
PUSH EDX
ADD EDX, 0
JE 0x0
SUB EDX, EBX
CALL 0x0
JMP 0x0
PUSH ESP
XOR ESP, EDX
JNE 0x0
PUSH EBP
PUSH EDX
```

```
CALL 0x0
```

74

72

FIG. 7

6/8

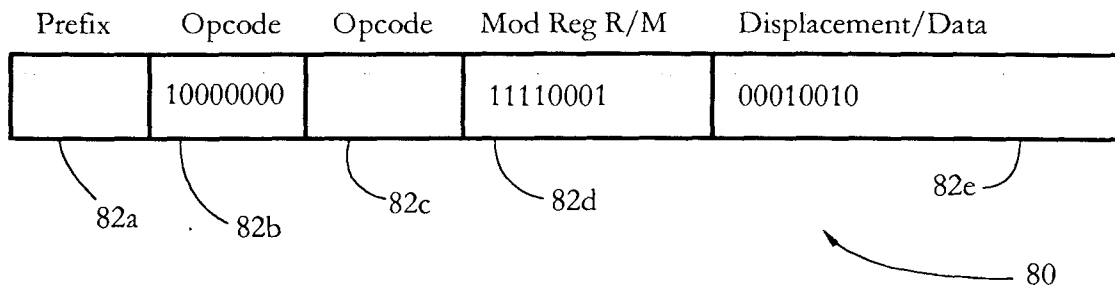


FIG. 8

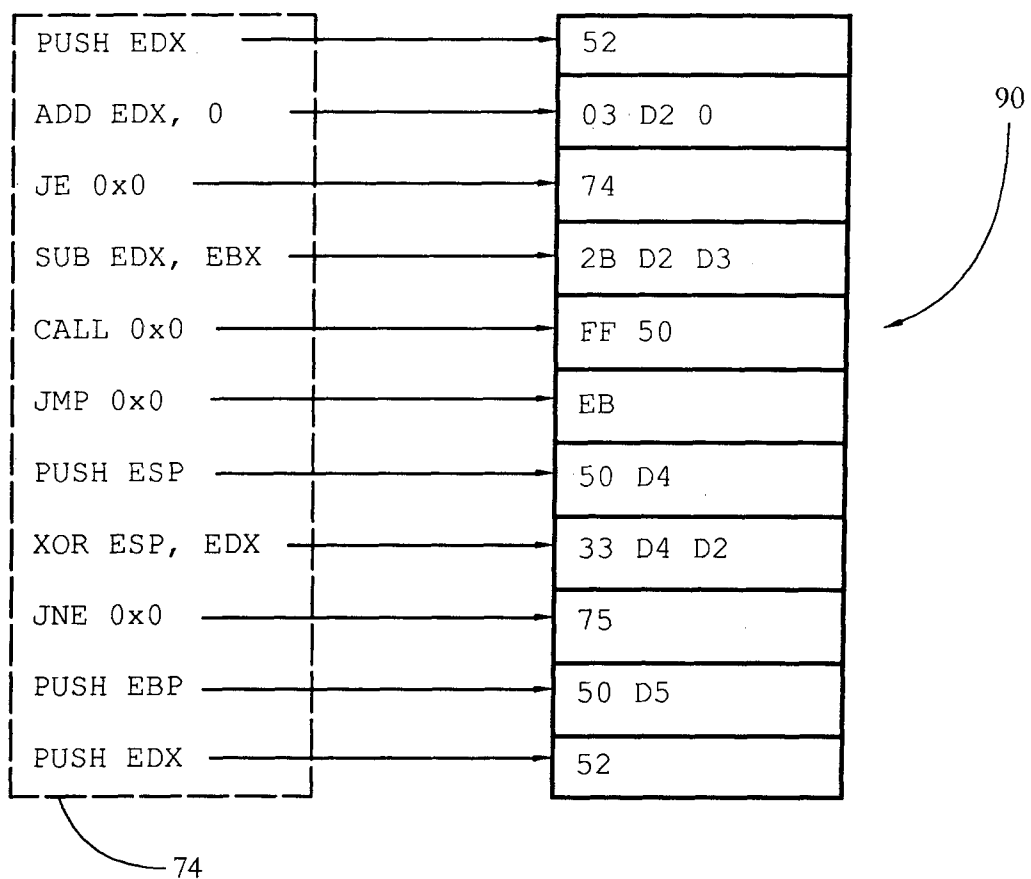


FIG. 9

7/8

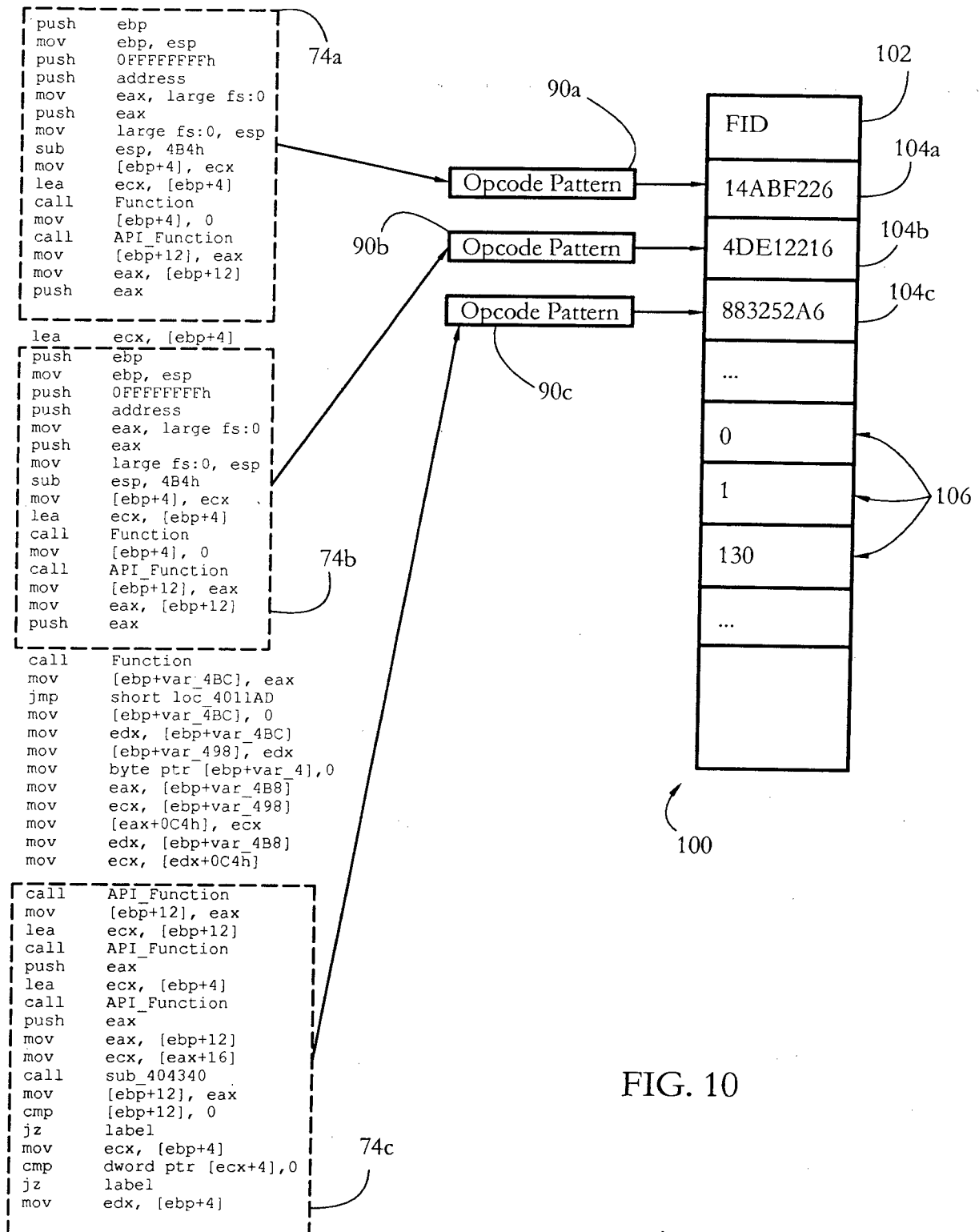


FIG. 10

8/8

FIG. 11

