```
400940 <tail_call_chain_1>:
    400940: 85 ff test %edi,%edi
    400942: 7e 08 jle 40094c
          <tail_call_chain_1+0xc>
    400944: 83 c7 ff add $0xffffffff,%edi
    400947: e9 14 01 00 00 jmpq 400a60
          <tail_call_chain_2>
    40094c: b8 2a 00 00 00 mov $0x2a,%eax
    400951: c3 retq
    400952: 66 2e 0f 1f 84 00 00 nopw
          %cs:0x0(%rax,%rax,1)
...
```

(a) Assembly code

```
400942 <FUNC_400940>:
    400940: 85 ff test %edi,%edi
    400942: 7e 08 jle 40094c
    400944: 83 c7 ff add $0xffffffff,%edi
400947 <FUNC_400947>:
    400947: e9 14 01 00 00 jmpq 400a60
40094c <FUNC_40094c>:
    40094c: b8 2a 00 00 00 mov $0x2a,%eax
    400951: c3 retq
    400952: 66 2e 0f 1f 84 00 00 nopw
          %cs:0x0(%rax,%rax,1)
...
```

(b) The output of disassembler with unsuitable forged FDEs.

```
FDE pc=40094c..400952
  DW_CFA_def_cfa: r7 (rsp) ofs 8
```

(c) FDE obfuscation success version

```
FDE pc=400947..40094c
  DW_CFA_nop
  DW_CFA_nop
  DW_CFA_nop
FDE pc=40094c..400952
  DW_CFA_def_cfa: r7 (rsp) ofs 8
```

(d) FDE obfuscation failed version

Fig. 12. An example for unsuitable forged FDEs (too close to the real function entry/ too many forged FDE)