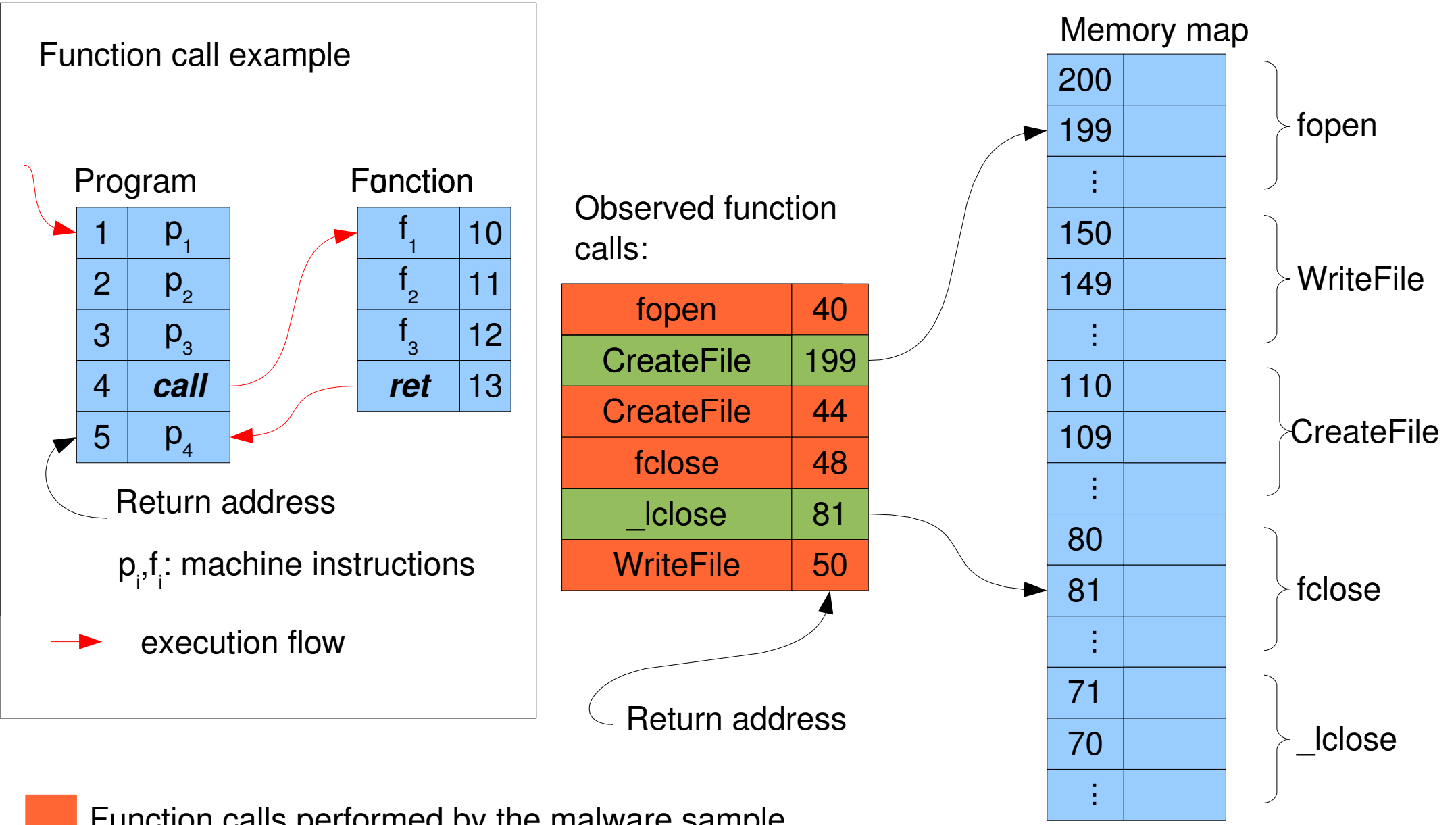
Function call example
Program
Function
1
p1
2
p2
3
p3
4
call
5
p4
f1
10
f2
11
f3
12
ret
13
Return address
pi,fi: machine instructions
execution flow
Observed function calls:
fopen
40
CreateFile
199
CreateFile
44
fclose
48
_lclose
81
WriteFile
50
Return address
Memory map
200
199
150
149
110
109
80
81
71
70
fopen
WriteFile
CreateFile
fclose
_lclose
Function calls performed by the malware sample
Function calls performed by the virtual operating system