```
5189: <bar>:
518d: pushq %rbp
......
51fa<foo>:
51b3: pushq %rbp
51b4: mov %rsp, %rbp
51b7: sub $0x10, %rsp
51bb: mov %rdi, -0x8(%rbp)
......
51d9: callq <bar>
......
51f4: callq <foo>
```

1. callq

$$\begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ \underline{|xxxxxxxx|} \leftarrow \%rsp \end{array} \quad \Rrightarrow \quad \begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ |xxxxxxxx| \\ \underline{|ret \quad addr|} \leftarrow \%rsp \end{array}$$

2. pushq %rbp

$$\begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ |xxxxxxxx| \\ \underline{|ret \quad addr|} \leftarrow \%rsp \end{array} \quad \Rrightarrow \quad \begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ |xxxxxxxx| \\ |ret \quad addr| \\ \underline{| \quad \%rbp \quad |} \leftarrow \%rsp \end{array}$$

3. mov %rsp, %rbp

$$\begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ |xxxxxxxx| \\ |ret \quad addr| \\ \underline{| \quad \%rbp \quad |} \leftarrow \%rsp \end{array} \quad \Rrightarrow \quad \begin{array}{l} |xxxxxxxx| \\ |xxxxxxxx| \\ |xxxxxxxx| \\ |ret \quad addr| \\ \underline{|origin\%rbp|} \leftarrow \%rsp, \%rbp \end{array}$$

4. sub $0x10, %rsp

$$\begin{array}{l} |xxxxxxxx| \leftarrow \%rbp \\ |xxxxxxxx| \\ |xxxxxxxx| \\ |ret \quad addr| \\ \underline{|origin\%rbp|} \leftarrow \%rsp, \%rbp \end{array} \quad \Rrightarrow \quad \begin{array}{l} |xxxxxxxx| \\ |xxxxxxxx| \\ |xxxxxxxx| \\ |ret \quad addr| \\ |origin\%rbp| \leftarrow \%rbp \\ |xxxxxxxx| \\ \underline{|xxxxxxxx|} \leftarrow \%rsp \end{array}$$

5. mov %rdi, -0x8(%rbp)

$$|xxxxxxxx| \leftarrow \%rbp \qquad |xxxxxxxx|$$

$$
\begin{array}{lcl}
|xxxxxxxx| & & |xxxxxxxx| \\
|xxxxxxxx| & & |xxxxxxxx| \\
|ret \quad addr| & & |ret \quad addr| \\
|origin\%rbp| \leftarrow \%rbp & & |origin\%rbp| \leftarrow \%rbp \\
|xxxxxxxx| & & |\quad \%rdi \quad| \\
\underline{|xxxxxxxx|} \leftarrow \%rsp & & \underline{|xxxxxxxx|} \leftarrow \%rsp
\end{array}
$$

6. callq

$$
\begin{array}{lcl}
|xxxxxxxx| \leftarrow \%rbp & & |xxxxxxxx| \\
|xxxxxxxx| & & |xxxxxxxx| \\
|xxxxxxxx| & & |xxxxxxxx| \\
|ret \quad addr| & & |ret \quad addr| \\
|origin\%rbp| \leftarrow \%rbp & & |origin\%rbp| \leftarrow \%rbp \\
|origin\%rdi| & & |origin\%rdi| \\
\underline{|xxxxxxxx|} \leftarrow \%rsp & & |xxxxxxxx| \\
 & & \underline{|ret \quad addr|} \leftarrow \%rsp
\end{array}
$$

7. pushq %rbp

$$
\begin{array}{lcl}
|xxxxxxxx| \leftarrow \%rbp & & |xxxxxxxx| \\
|xxxxxxxx| & & |xxxxxxxx| \\
|xxxxxxxx| & & |xxxxxxxx| \\
|ret \quad addr| & & |ret \quad addr| \\
|origin\%rbp| \leftarrow \%rbp & & |origin\%rbp| \leftarrow \%rbp \\
|origin\%rdi| & & |origin\%rdi| \\
|xxxxxxxx| & & |xxxxxxxx| \\
\underline{|ret \quad addr|} \leftarrow \%rsp & & |ret \quad addr| \\
 & & \underline{|\quad \%rbp \quad|} \leftarrow \%rsp
\end{array}
$$

$Stack\ before\ 518e:$

$0xfe2f8 \rightarrow |ret \quad addr|$

$0xfe2f0 \rightarrow |origin\%rbp| \leftarrow \%rbp$

$0xfe2e8 \rightarrow |origin\%rdi|$

$0xfe2e0 \rightarrow |xxxxxxxx|$

$0xfe2d8 \rightarrow |ret \quad addr|$

$0xfe2d0 \rightarrow \underline{|\quad \%rbp \quad|} \leftarrow \%rsp$