C stack – possible error

```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}
```

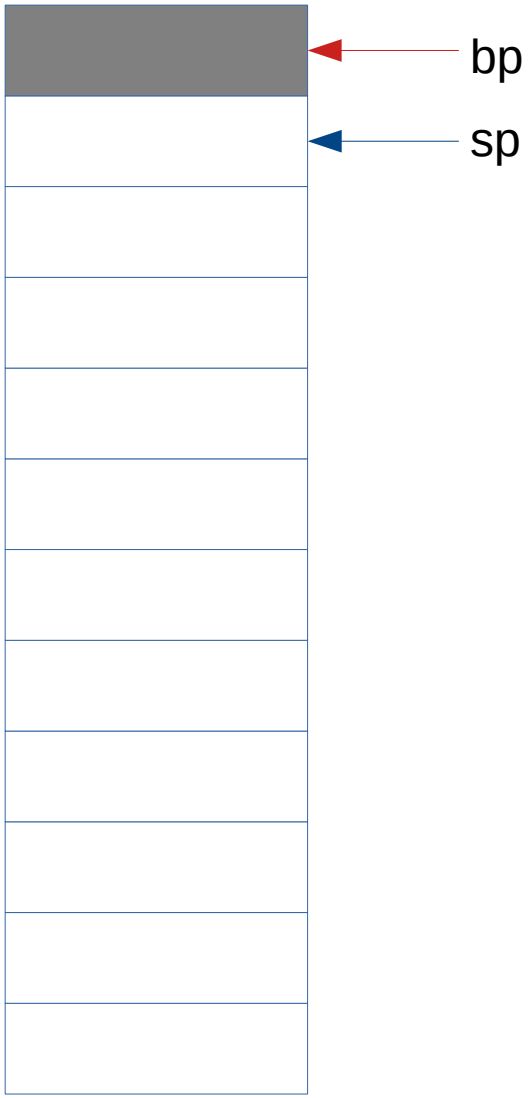
```
char *answer( char *question)
{
   char buffer[20];
   printf(”%s ”, question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf(”%s ”, question);
   gets(buffer);
   return buffer;
}
```

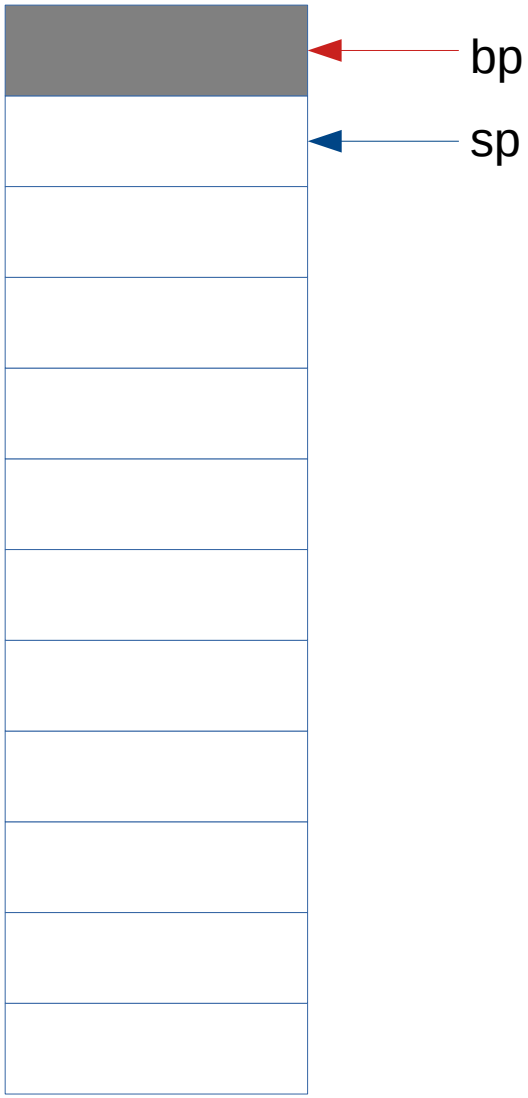


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf(”%s ”, question);
   gets(buffer);
   return buffer;
}
```

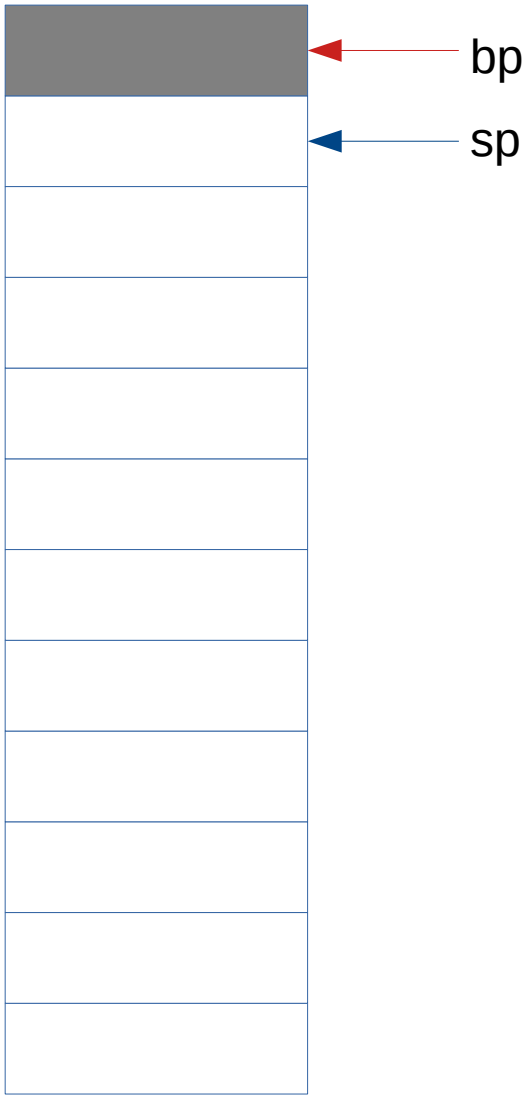


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

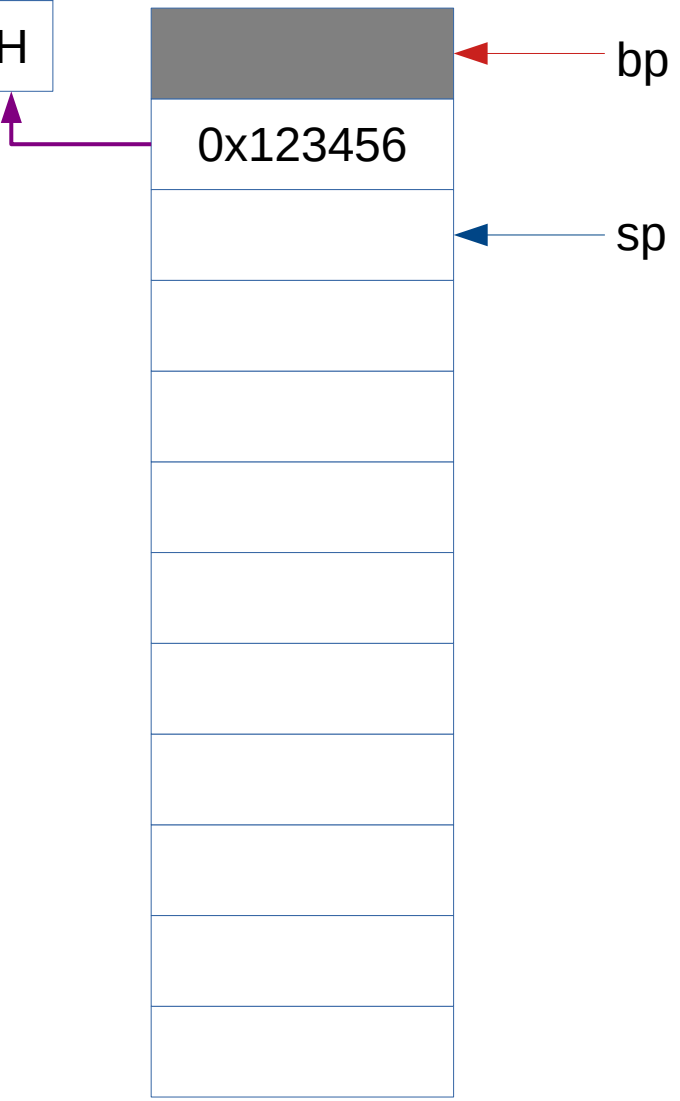
```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf(”%s ”, question);
   gets(buffer);
   return buffer;
}
```



.rodata

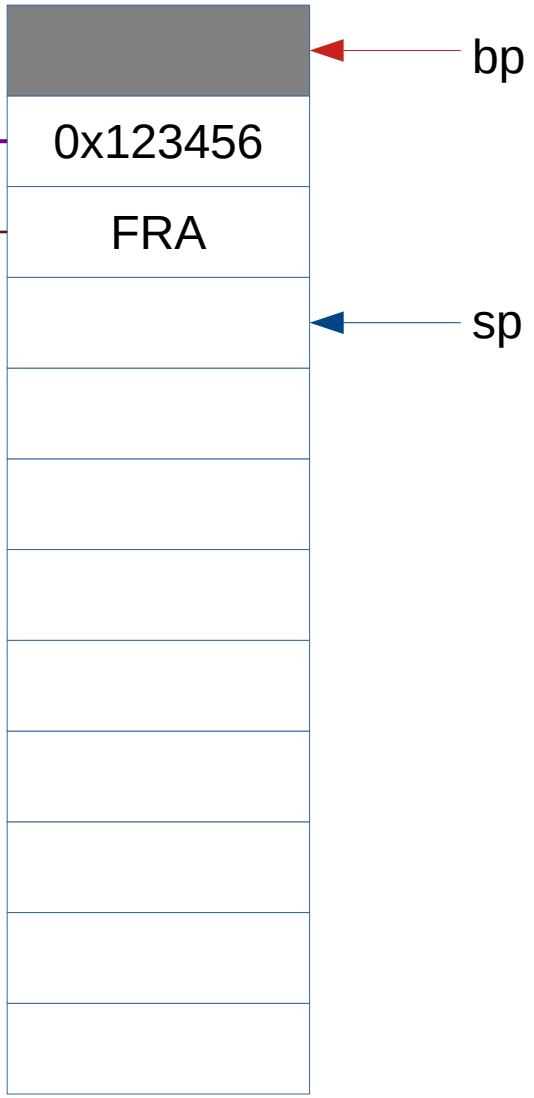
\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H




```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}



char *answer( char *question)
{
   char buffer[20];
   printf(”%s ”, question);
   gets(buffer);
   return buffer;
}
```

.rodata

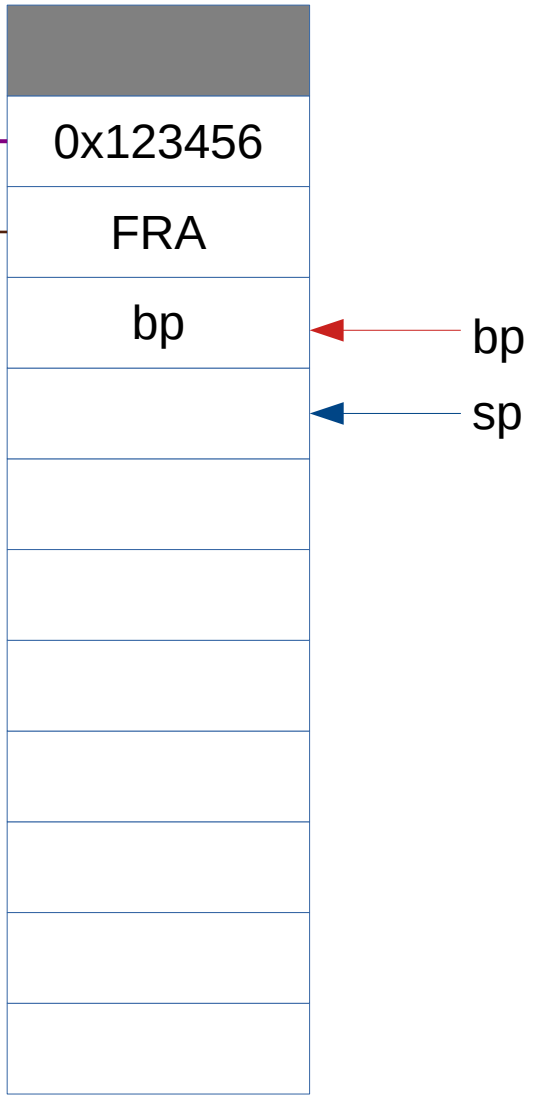
\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H




```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}



char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

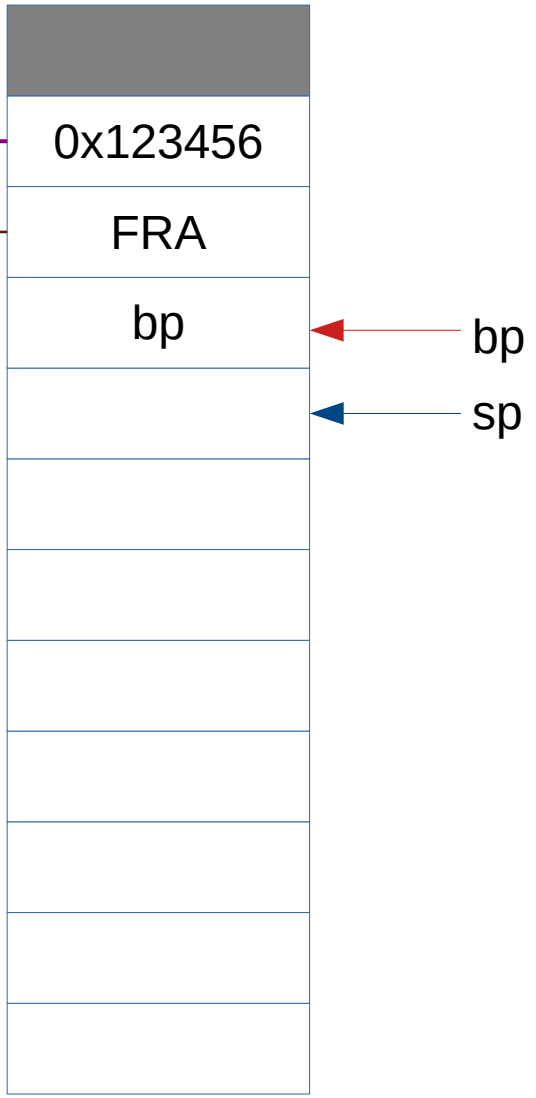



```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

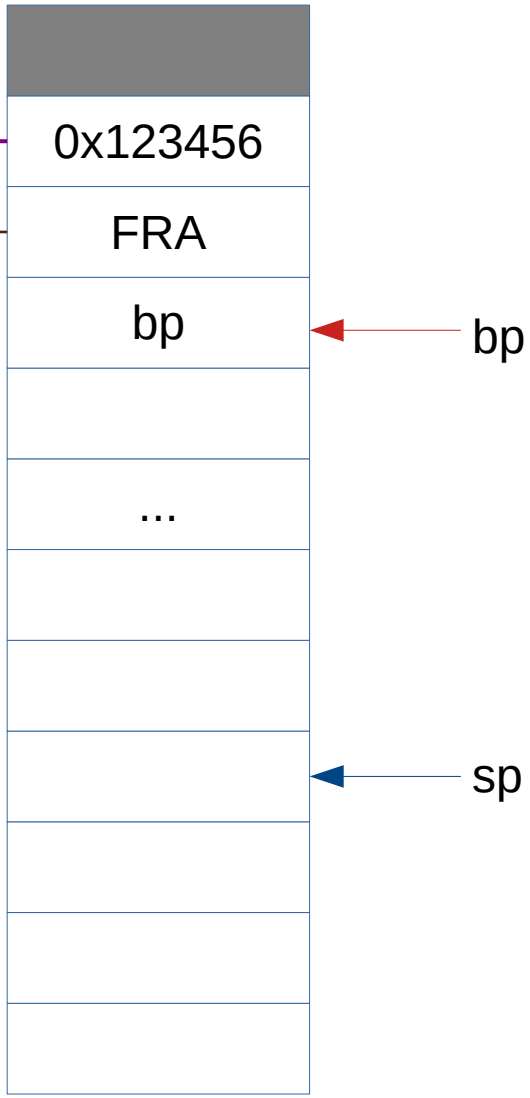



```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

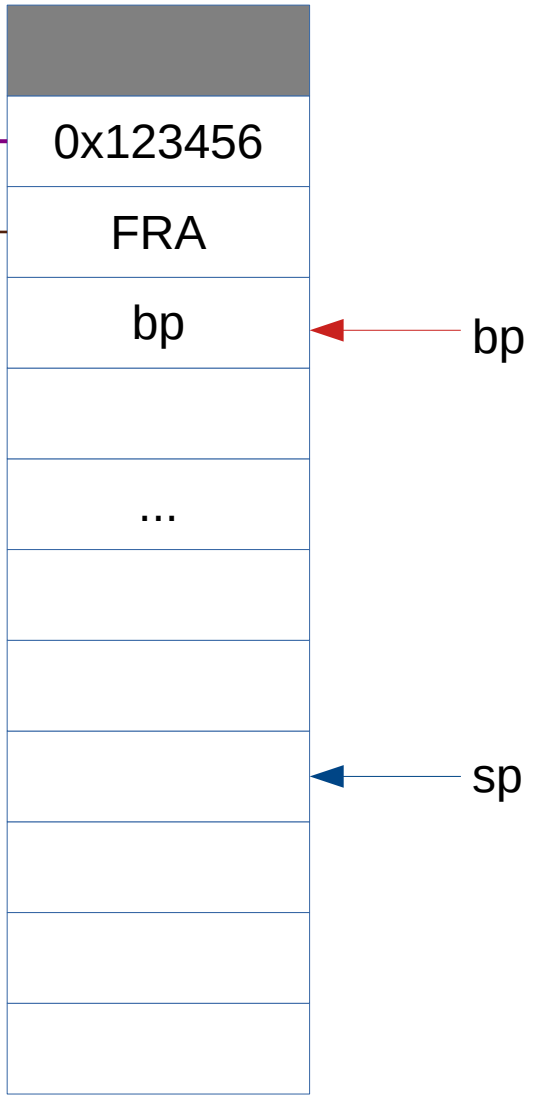



```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H




```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

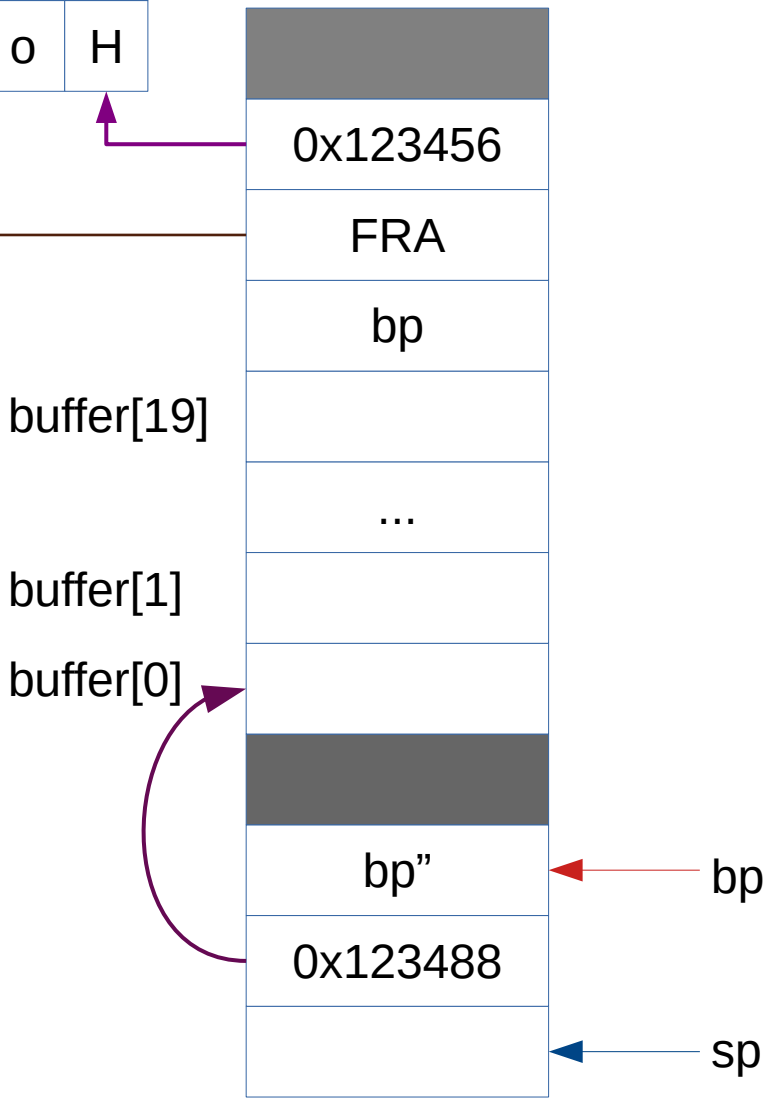
```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   gets(buffer);
   return buffer;
}
```

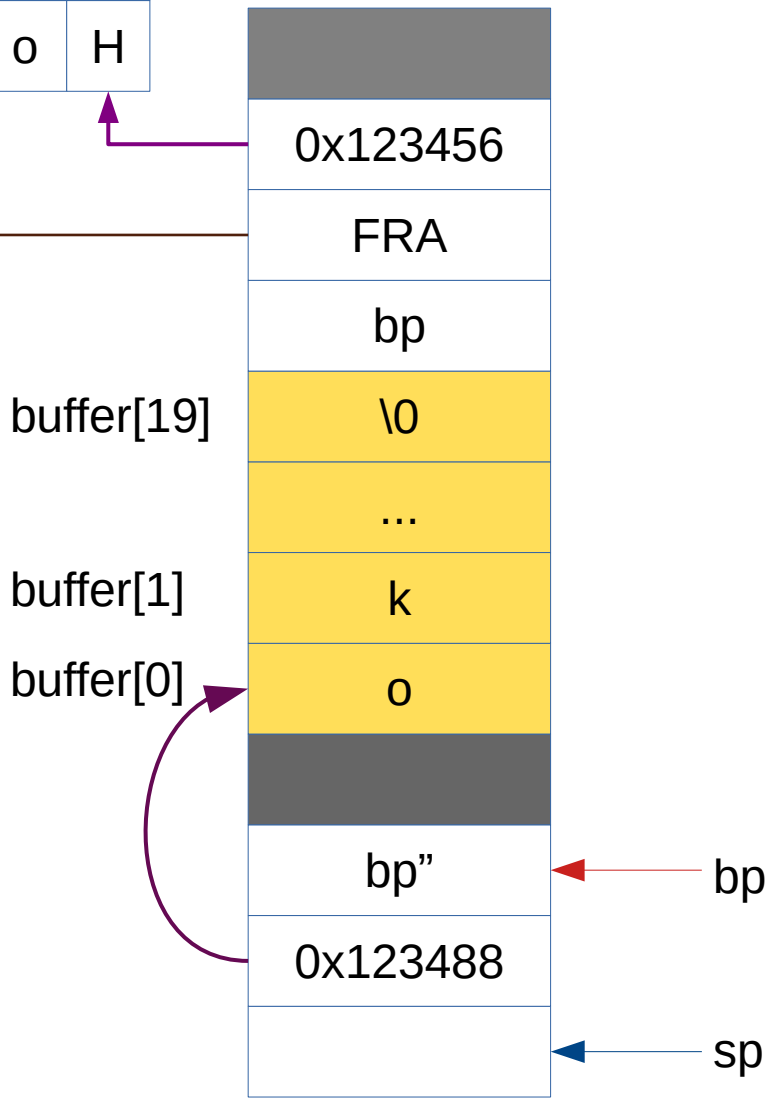


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    gets(buffer);
    return buffer;
}
```

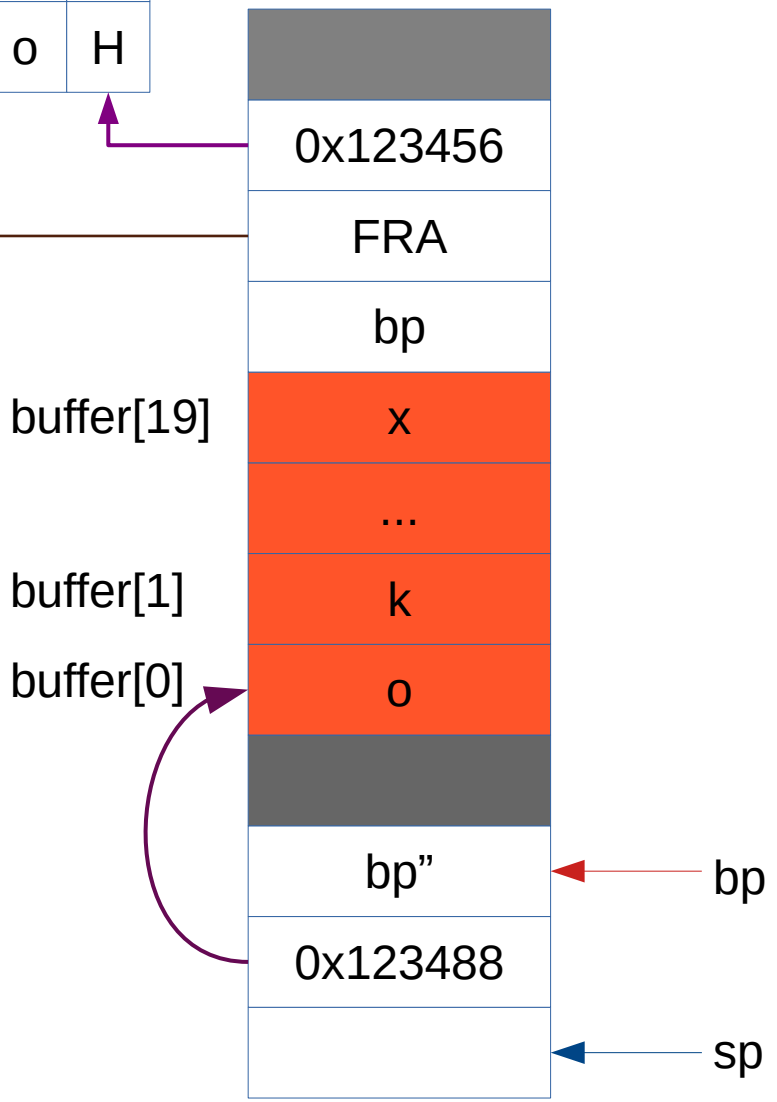


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
         answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    gets(buffer);
    return buffer;
}
```

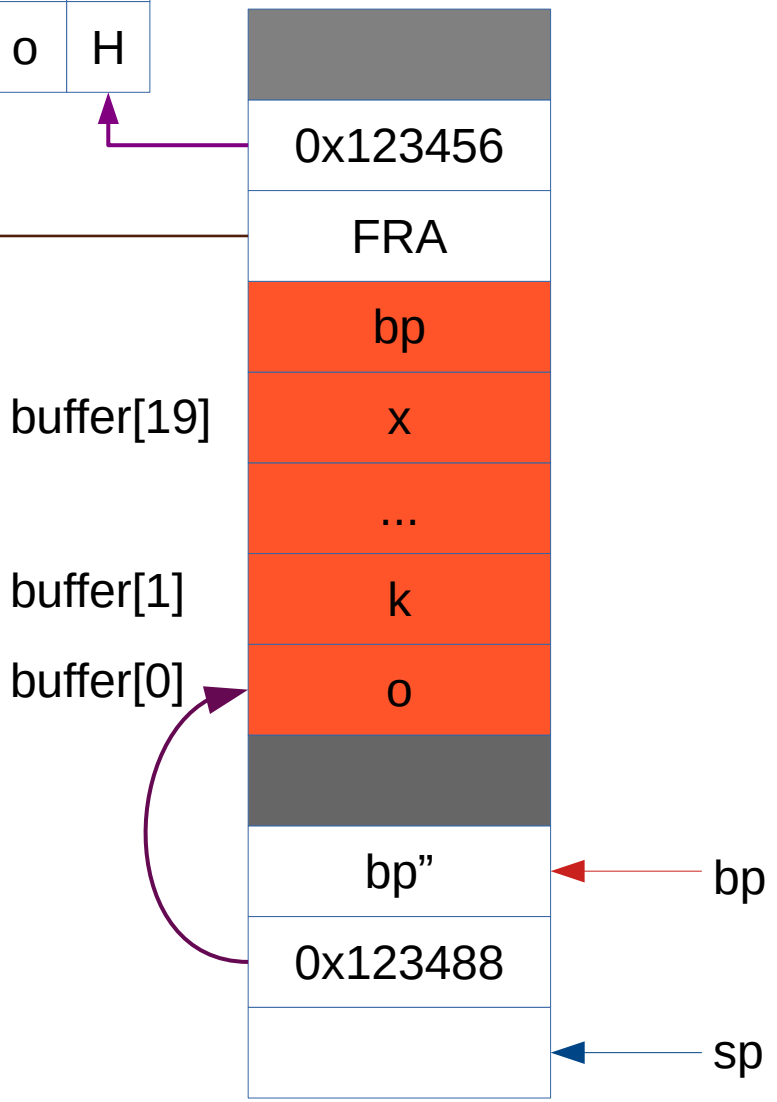


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
         answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    gets(buffer);
    return buffer;
}
```

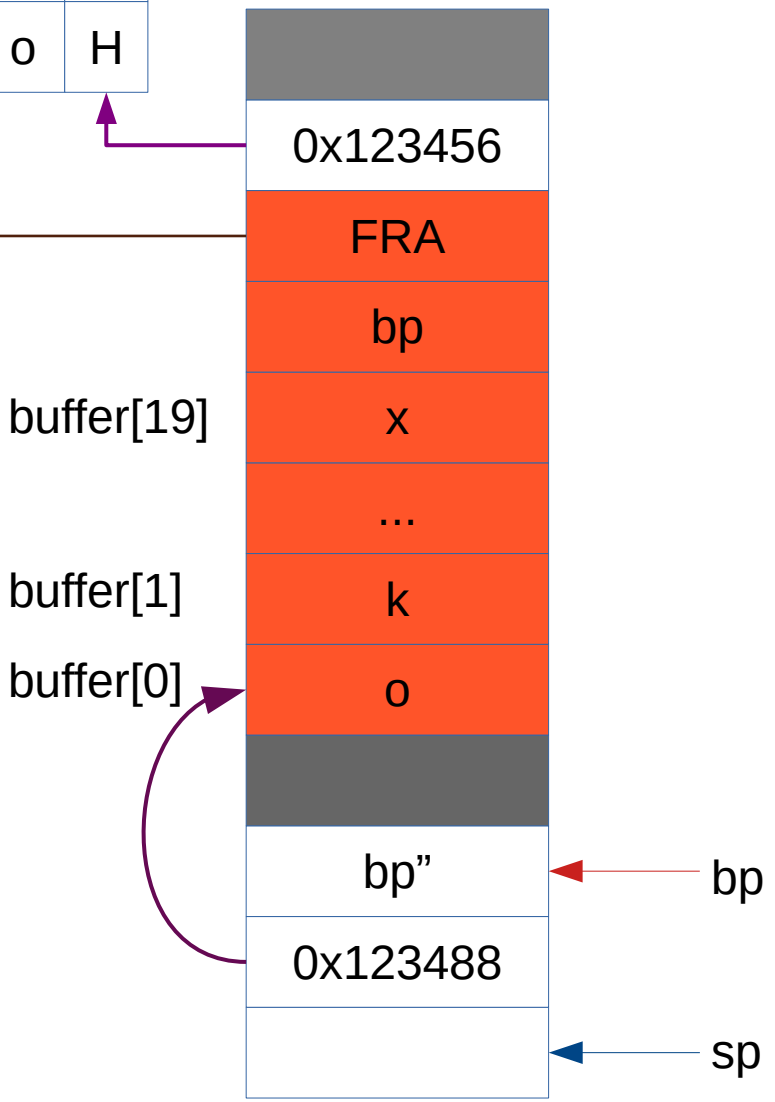


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
         answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    gets(buffer);
    return buffer;
}
```

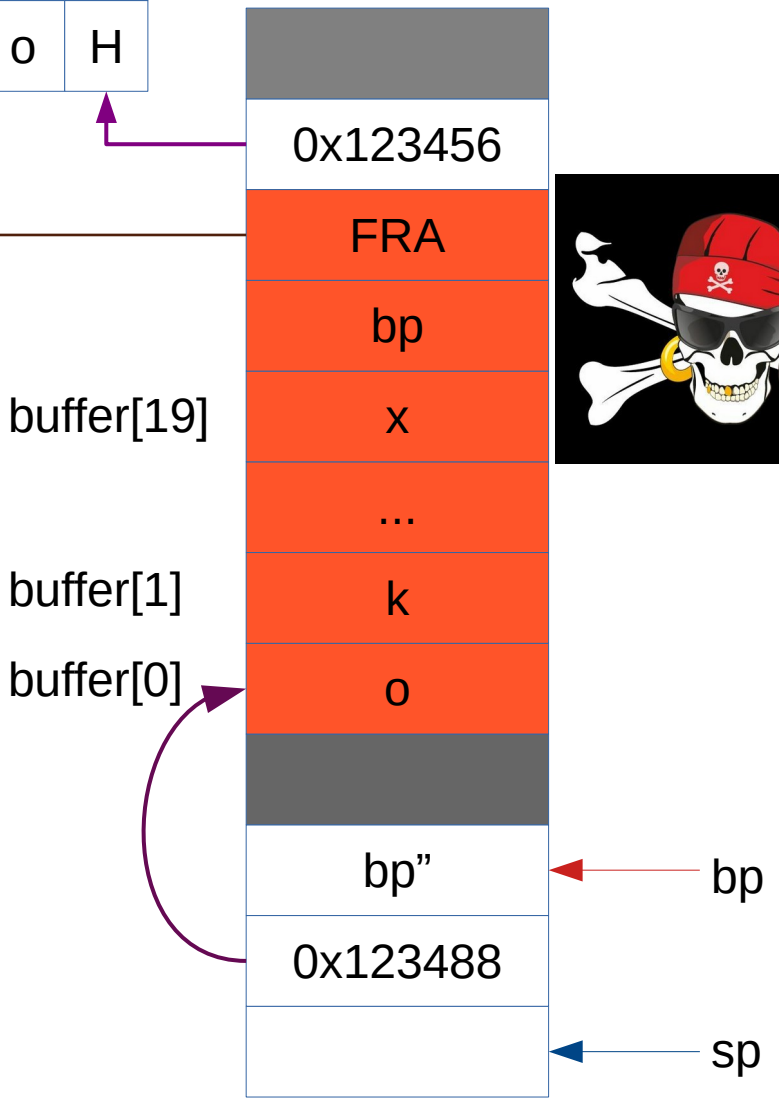


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    gets(buffer);
    return buffer;
}
```



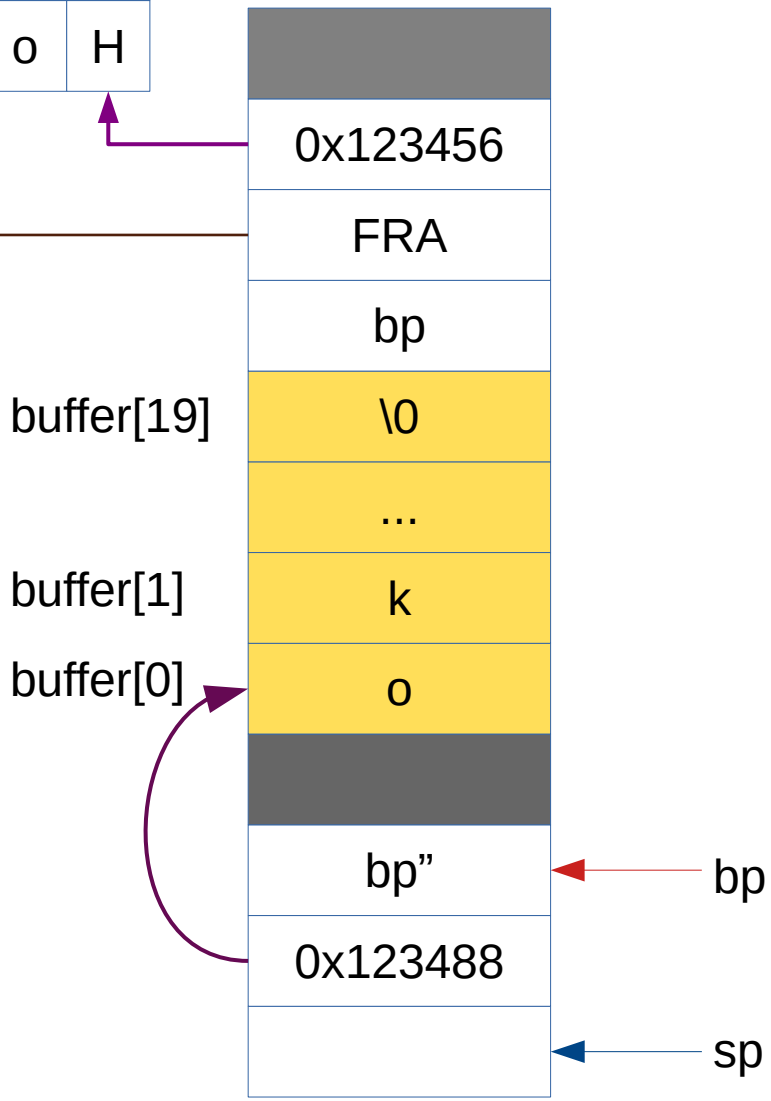
BUFFER OVERFLOW!

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
         answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    fgets(buffer,20,stdin);
    return buffer;
}
```

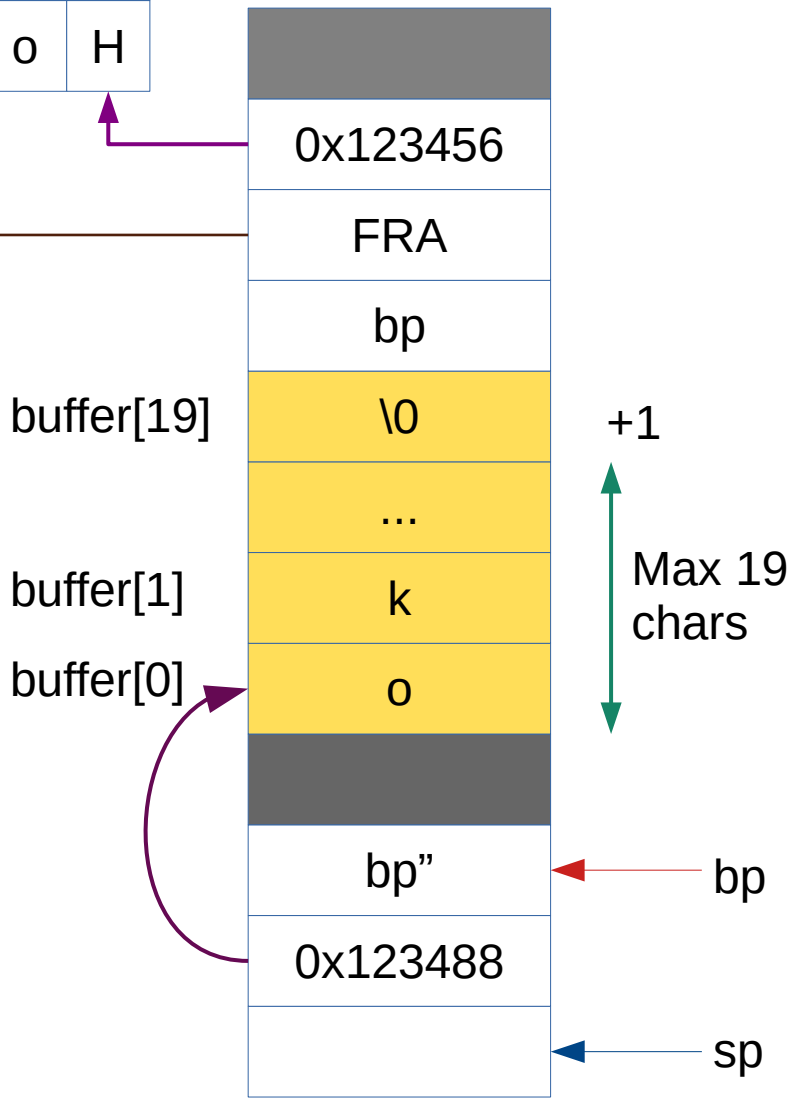


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    fgets(buffer,20,stdin);
    return buffer;
}
```

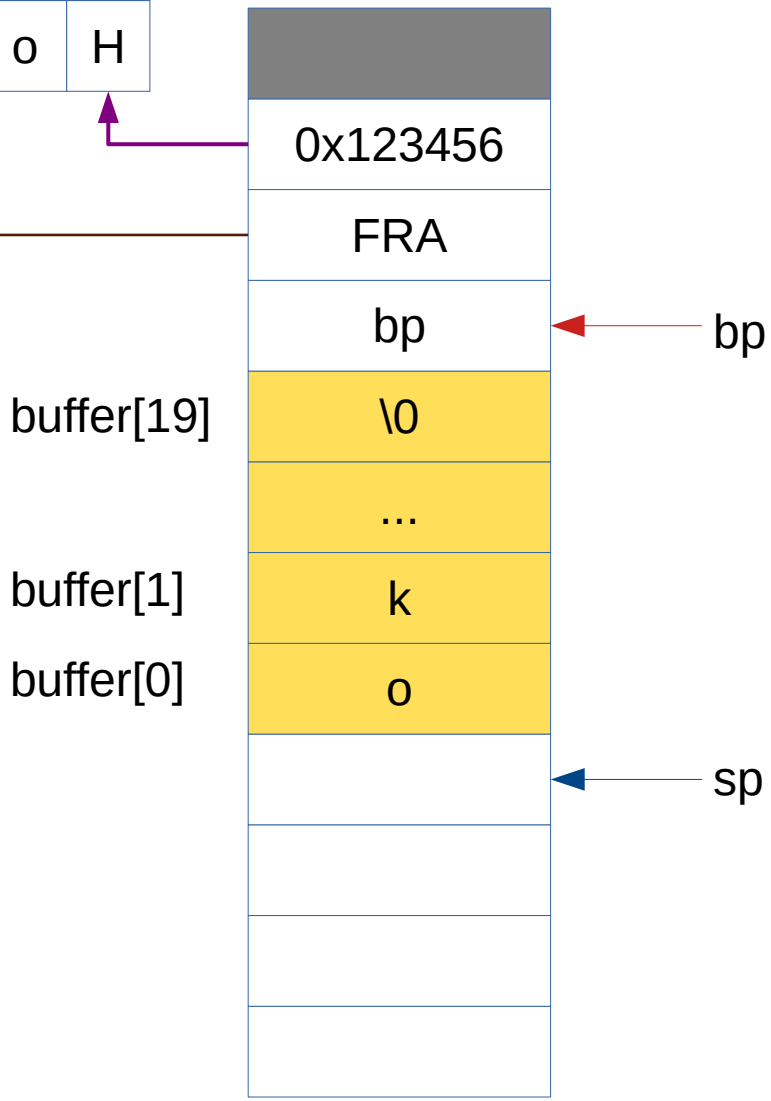


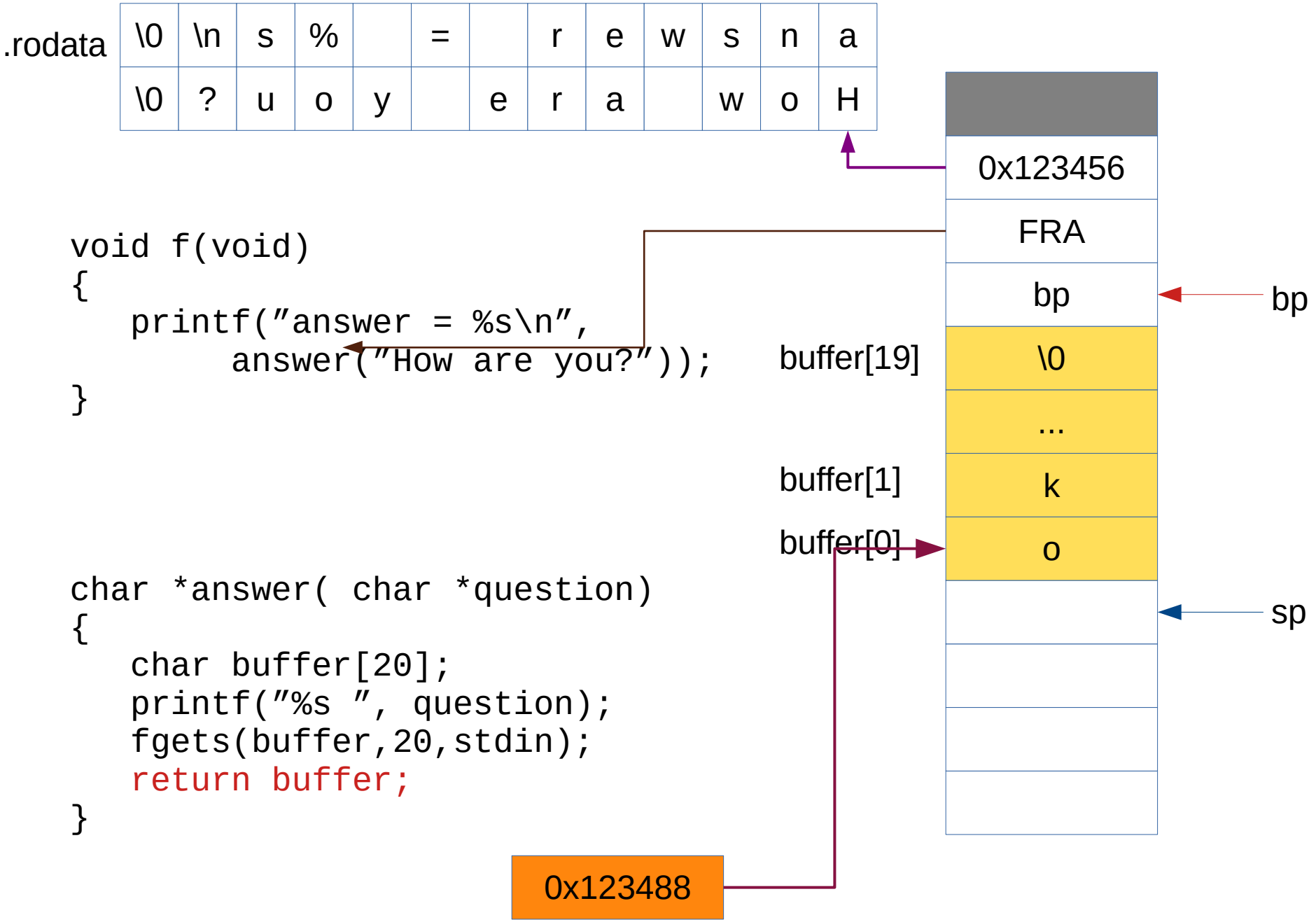
.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



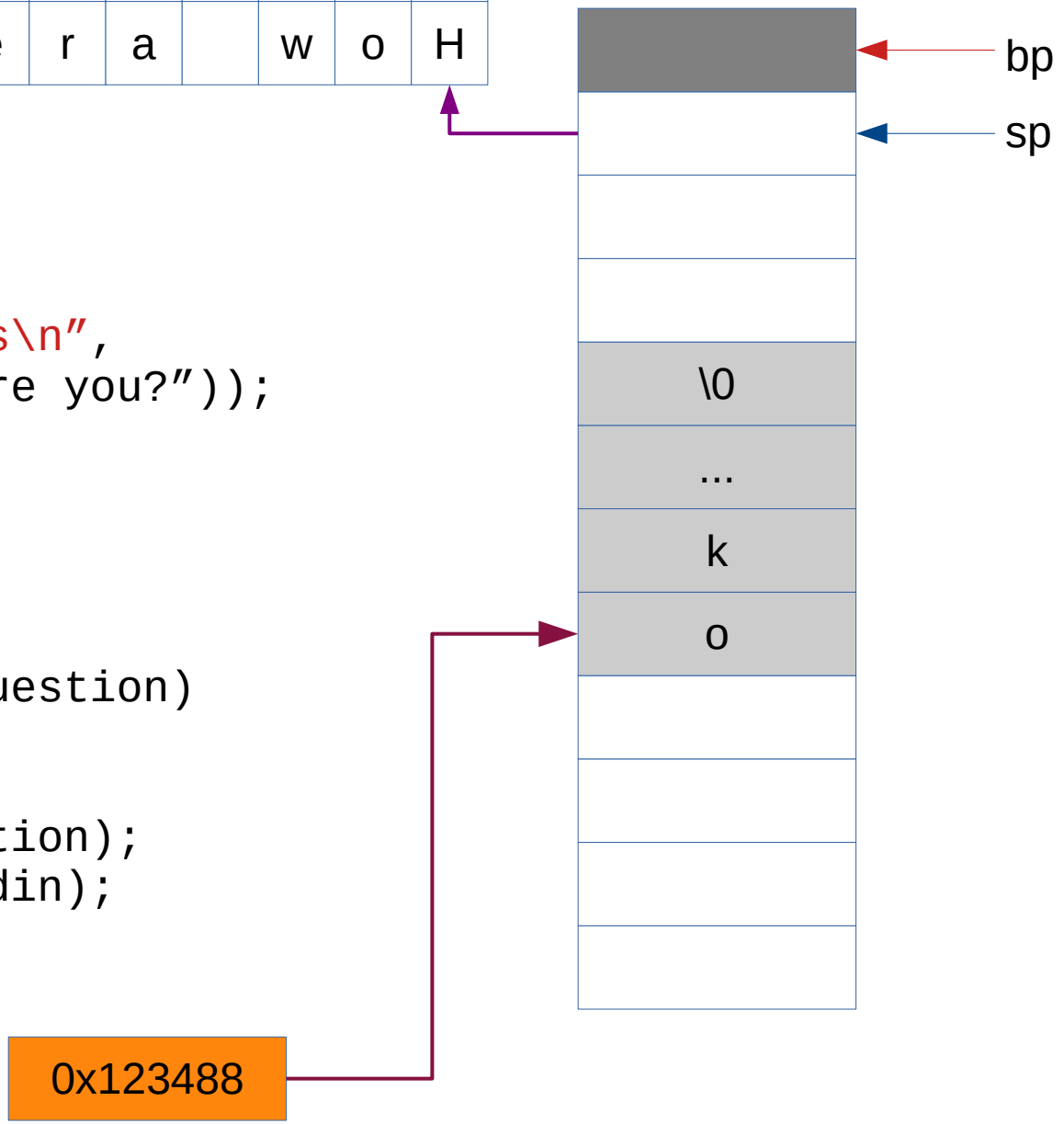

.rodata
\0 \n s % = r e w s n a
\0 ? u o y e r a w o H
0x123456
FRA
bp
bp
buffer[19]
\0
...
buffer[1]
k
buffer[0]
o
sp
0x123488
void f(void)
{
printf("answer = %s\n",
answer("How are you?"));
}
char *answer(char *question)
{
char buffer[20];
printf("%s ", question);
fgets(buffer,20,stdin);
return buffer;
}

.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}
```

```
char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

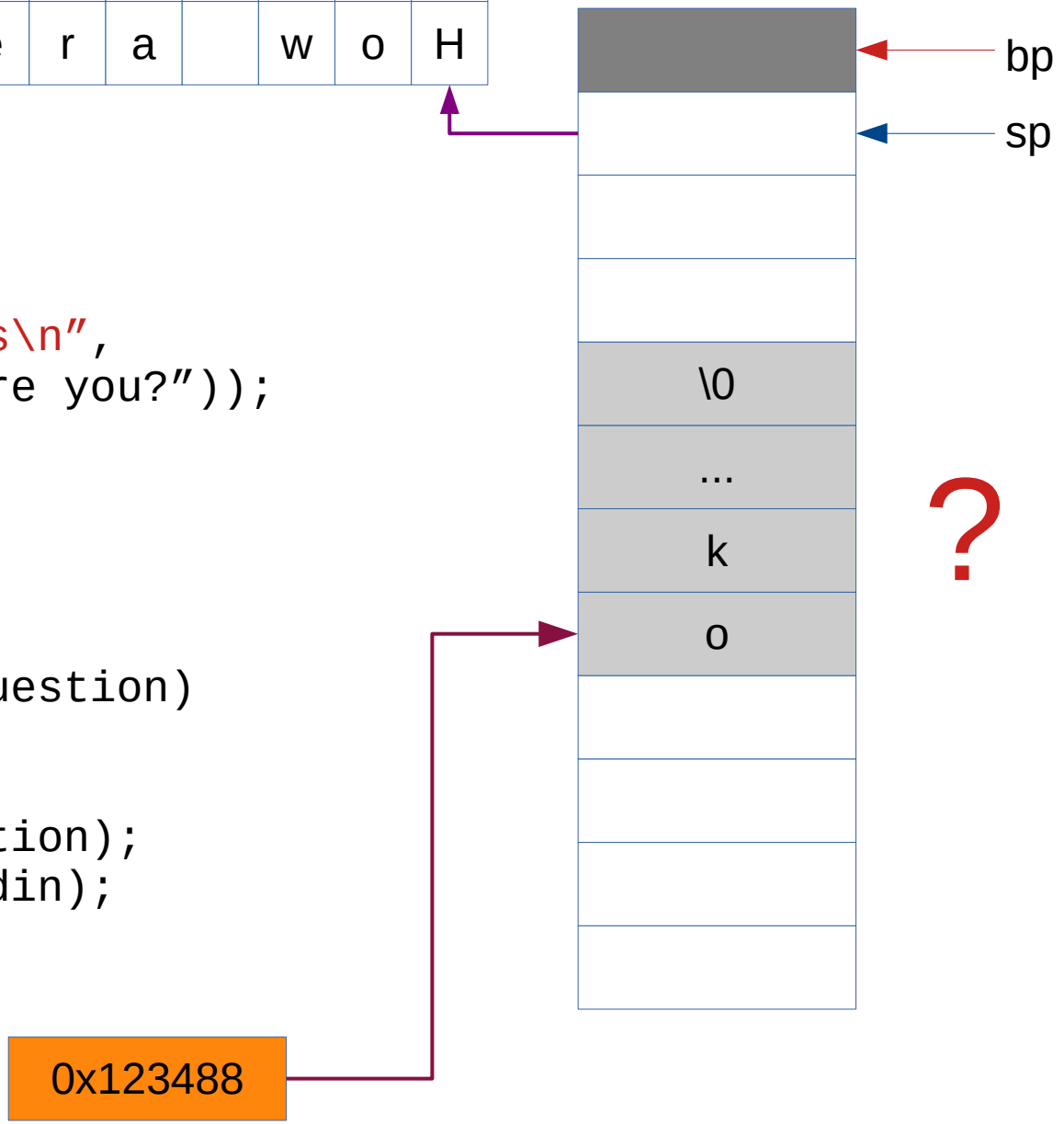


.rodata

\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

```
void f(void)
{
    printf("answer = %s\n",
         answer("How are you?"));
}
```

```
char *answer( char *question)
{
    char buffer[20];
    printf("%s ", question);
    fgets(buffer,20,stdin);
    return buffer;
}
```

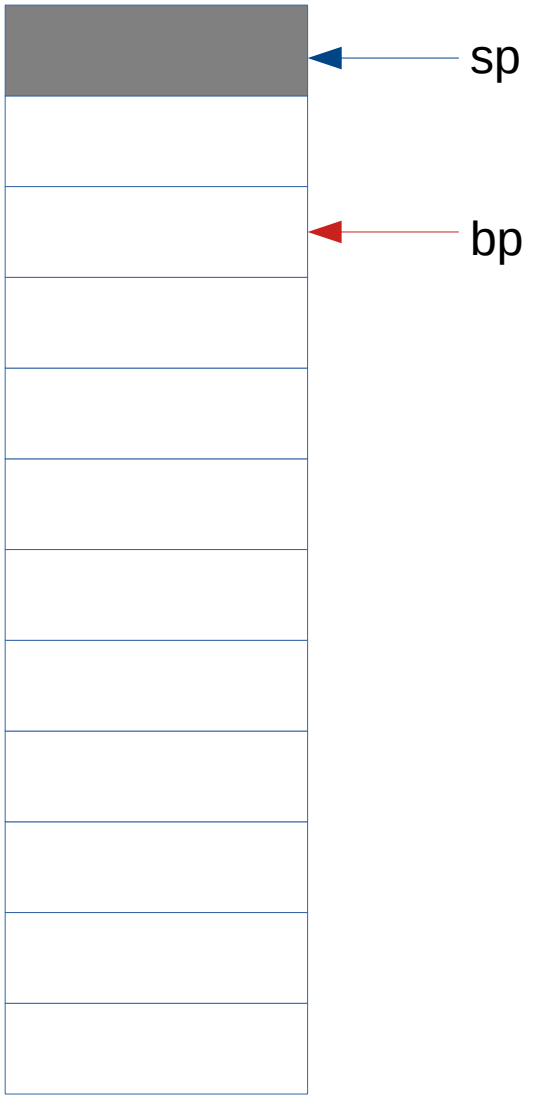


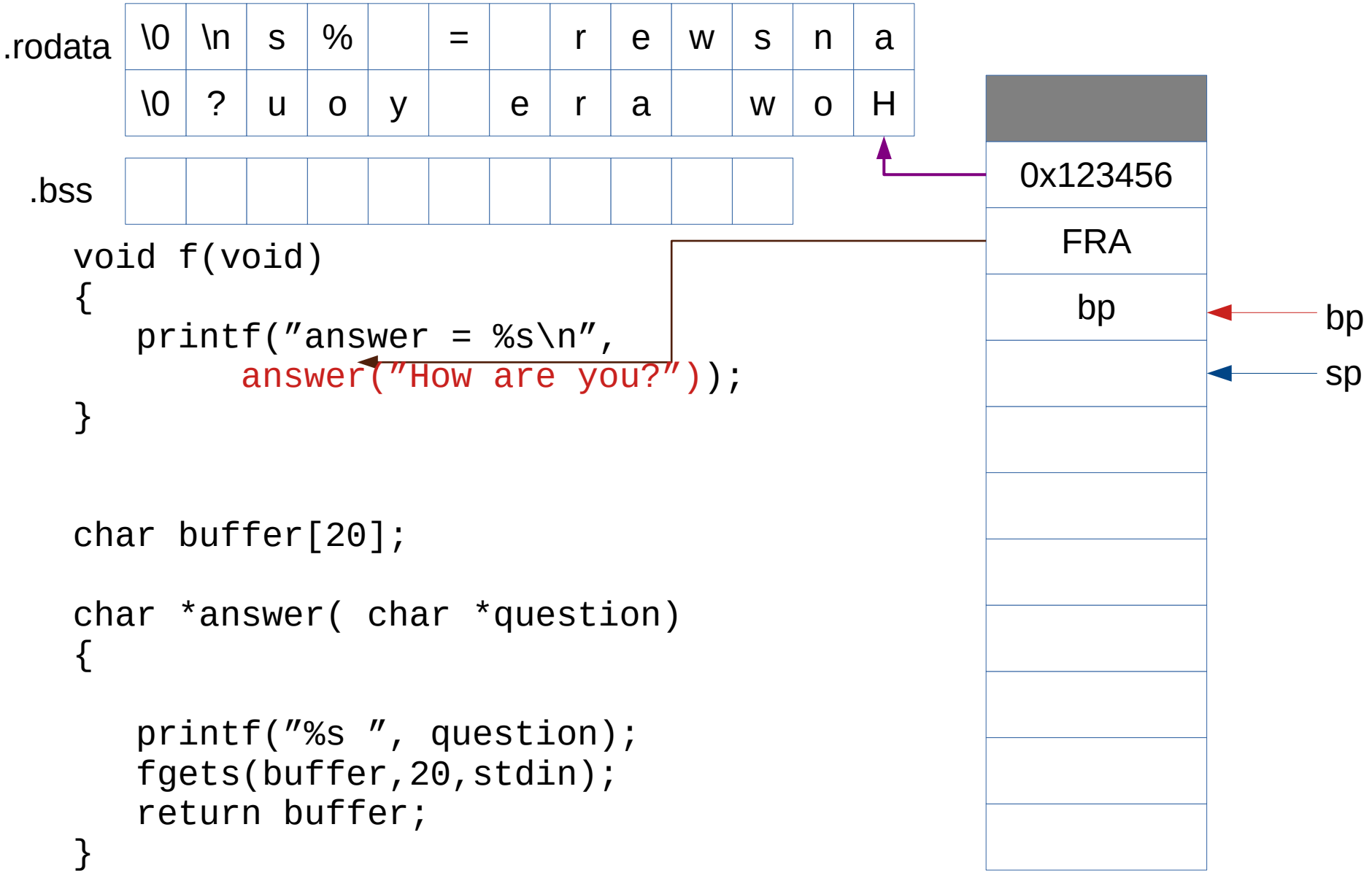
.rodata

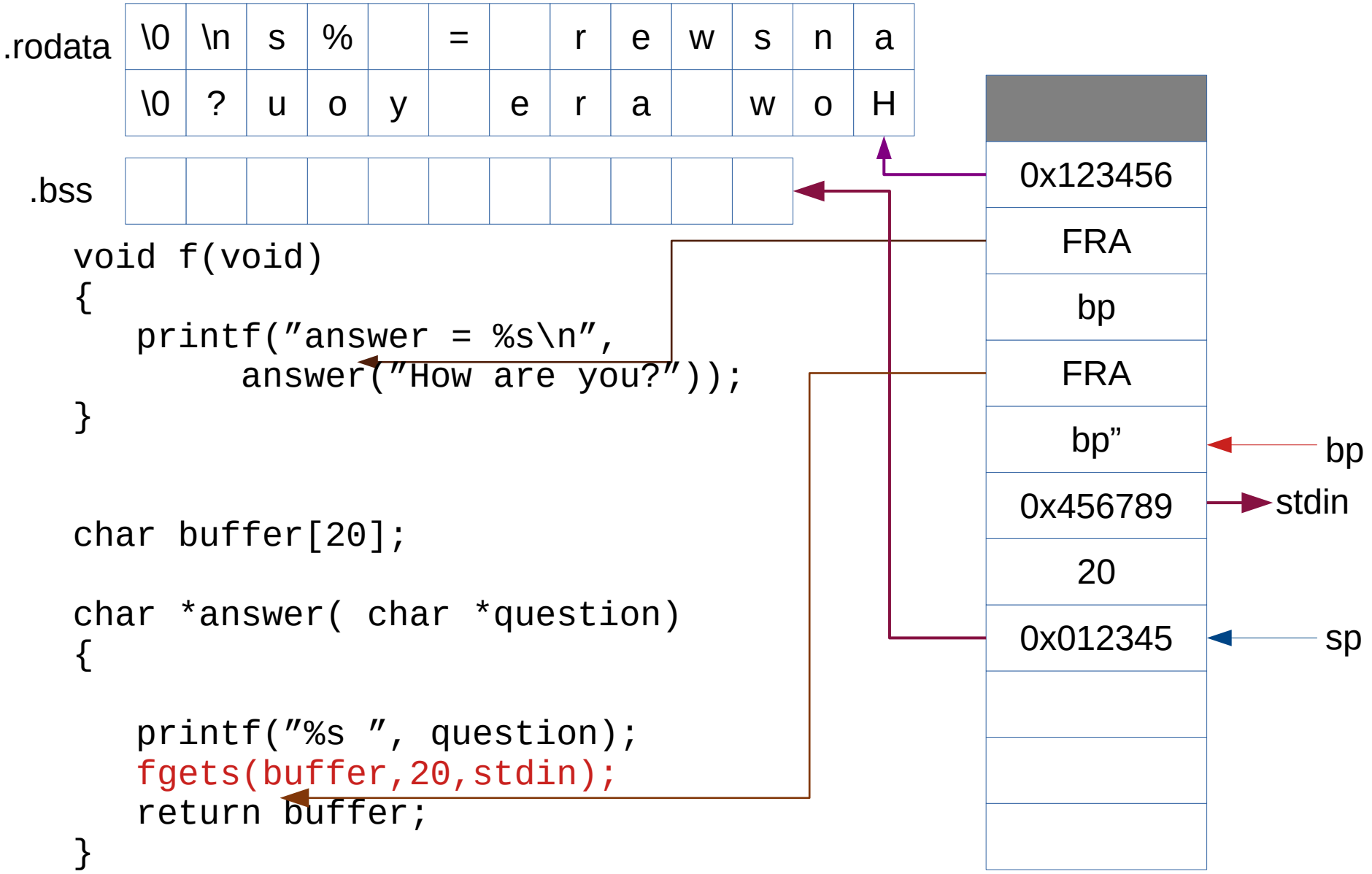
\0	\n	s	%		=		r	e	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

.bss

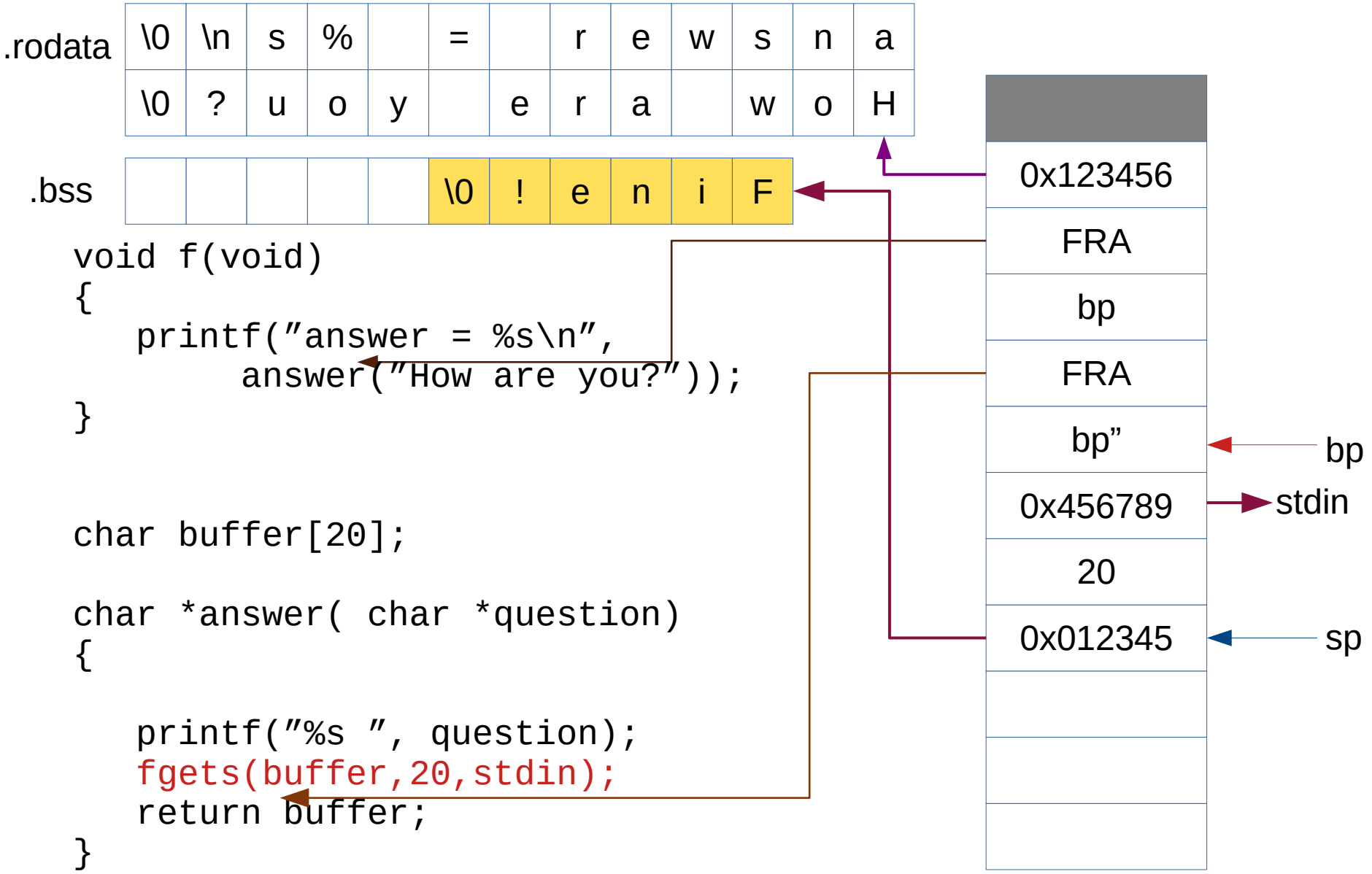

```
void f(void)
{
   printf("answer = %s\n",
        answer("How are you?"));
}


char buffer[20];

char *answer( char *question)
{
   char buffer[20];
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



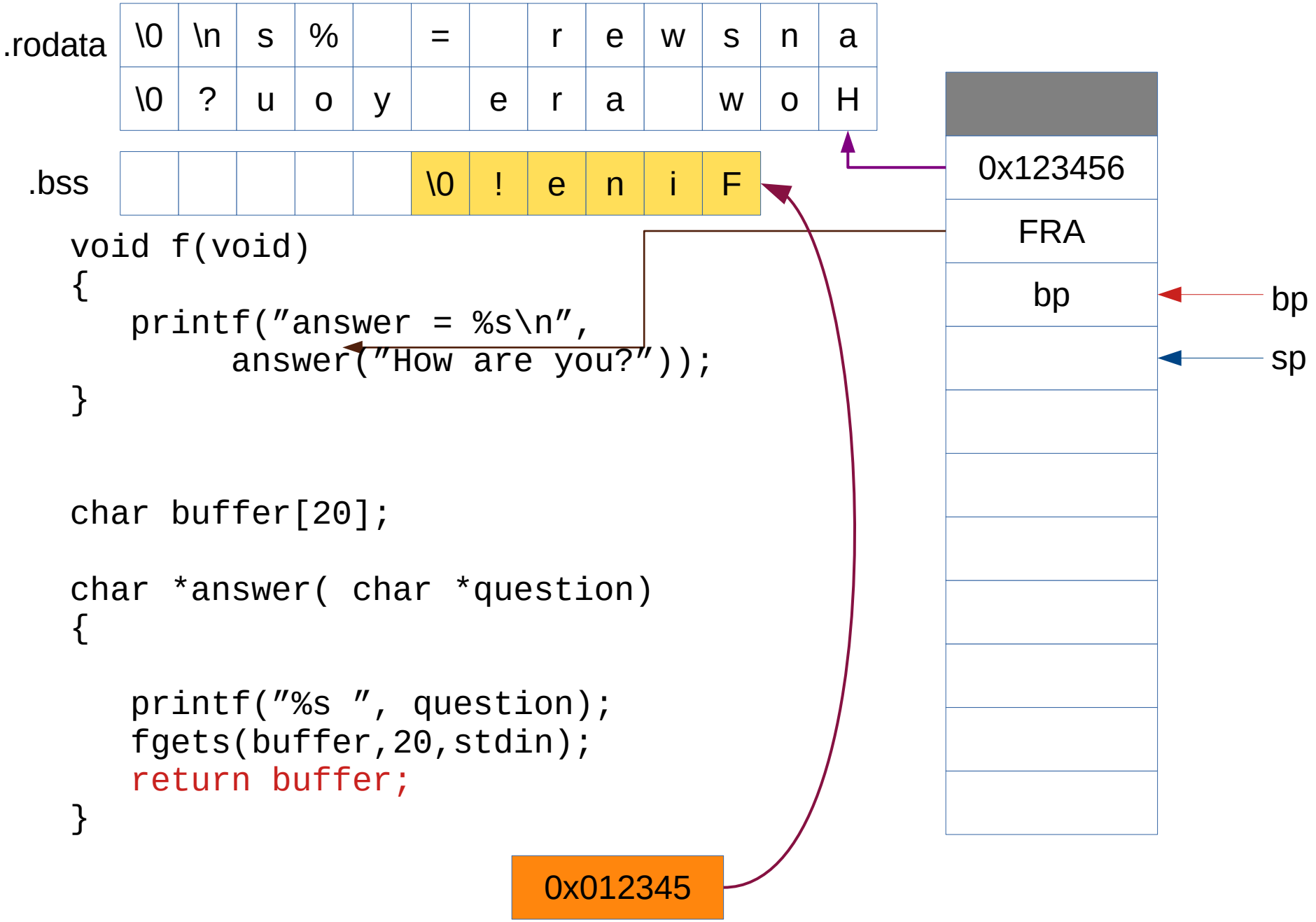

.rodata
\0 \n s % = r e w s n a
\0 ? u o y e r a w o H
.bss
0x123456
FRA
bp
bp
sp
void f(void)
{
printf("answer = %s\n",
answer("How are you?"));
}
char buffer[20];
char *answer(char *question)
{
printf("%s ", question);
fgets(buffer,20,stdin);
return buffer;
}



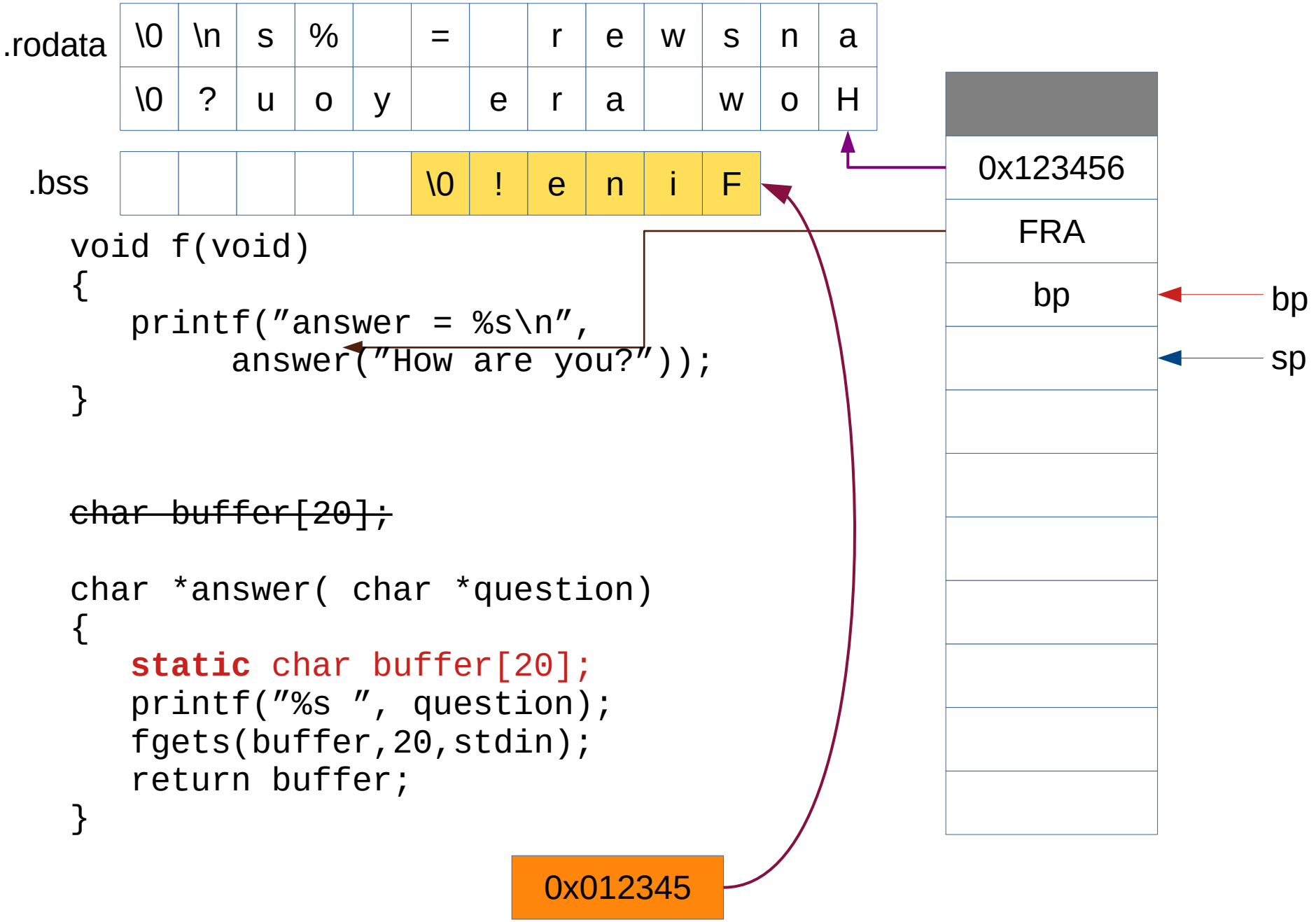

```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}


char buffer[20];

char *answer( char *question)
{

   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```




```
void f(void)
{
   printf(”answer = %s\n”,
        answer(”How are you?”));
}


char buffer[20];

char *answer( char *question)
{

   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```




```
void f(void)
{
    printf("answer = %s\n",
        answer("How are you?"));
}


char buffer[20];

char *answer( char *question)
{

    printf("%s ", question);
    fgets(buffer,20,stdin);
    return buffer;
}
```



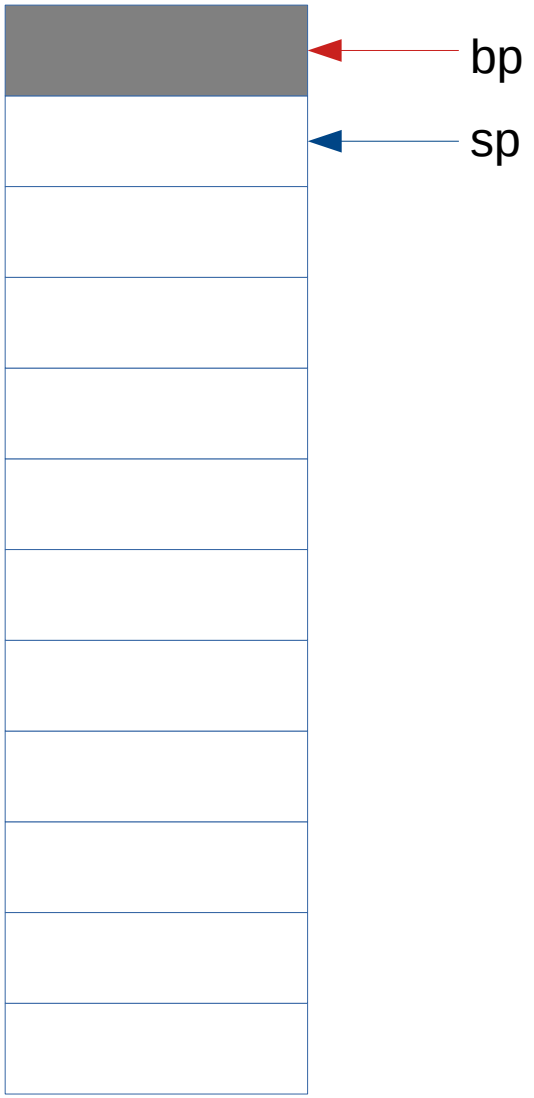

```
void f(void)
{
    printf("answer = %s\n",
        answer("How are you?"));
}


char buffer[20];

char *answer( char *question)
{
    static char buffer[20];
    printf("%s ", question);
    fgets(buffer,20,stdin);
    return buffer;
}
```

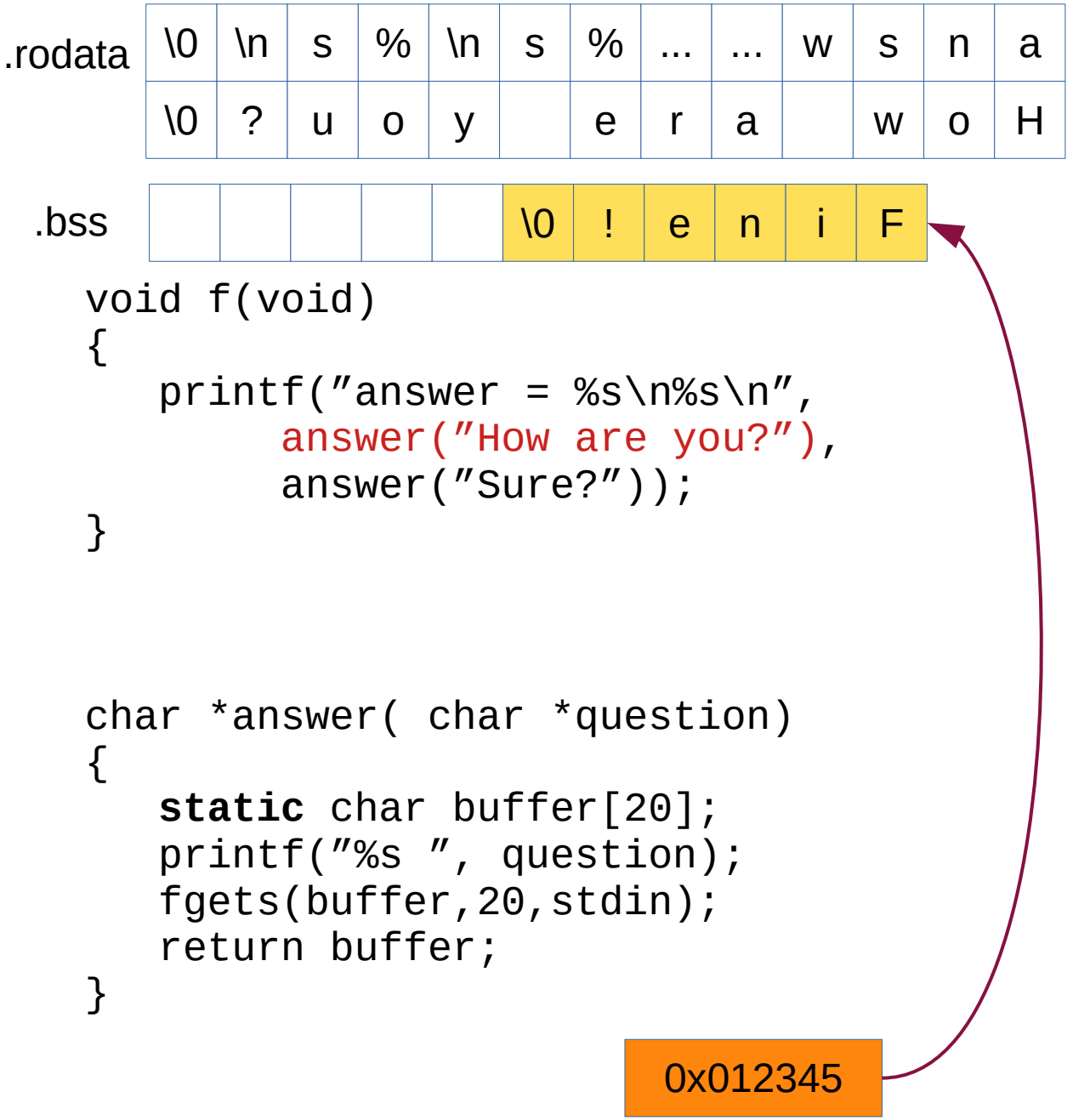
.rodata

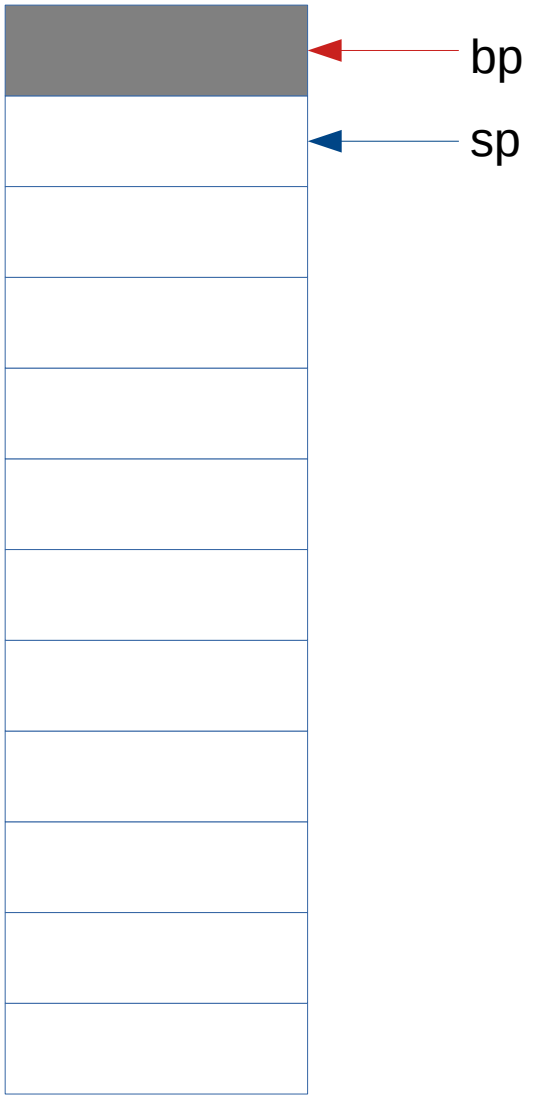
\0	\n	s	%	\n	s	%	...	...	w	s	n	a
\0	?	u	o	y		e	r	a		w	o	H

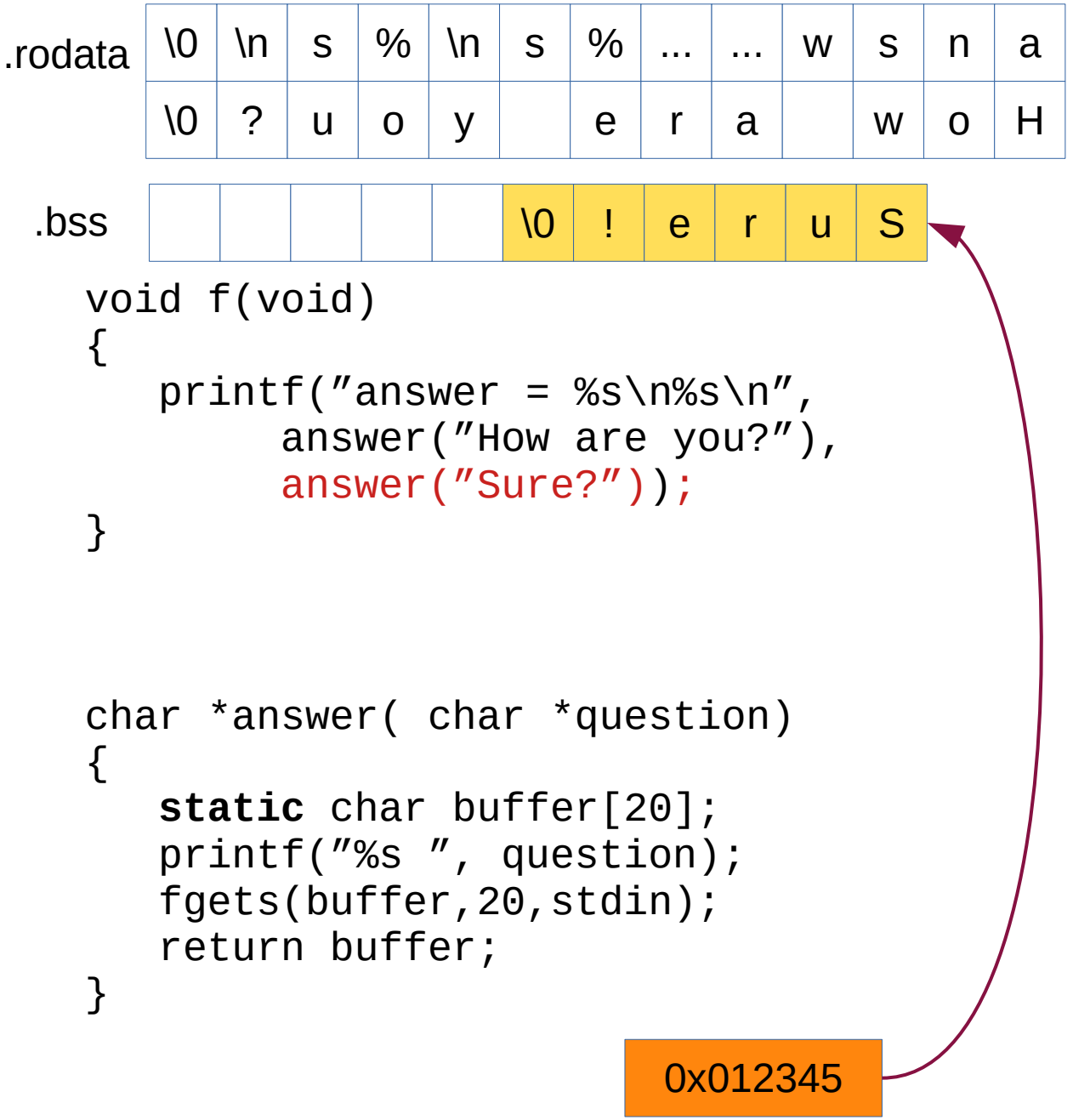
.bss

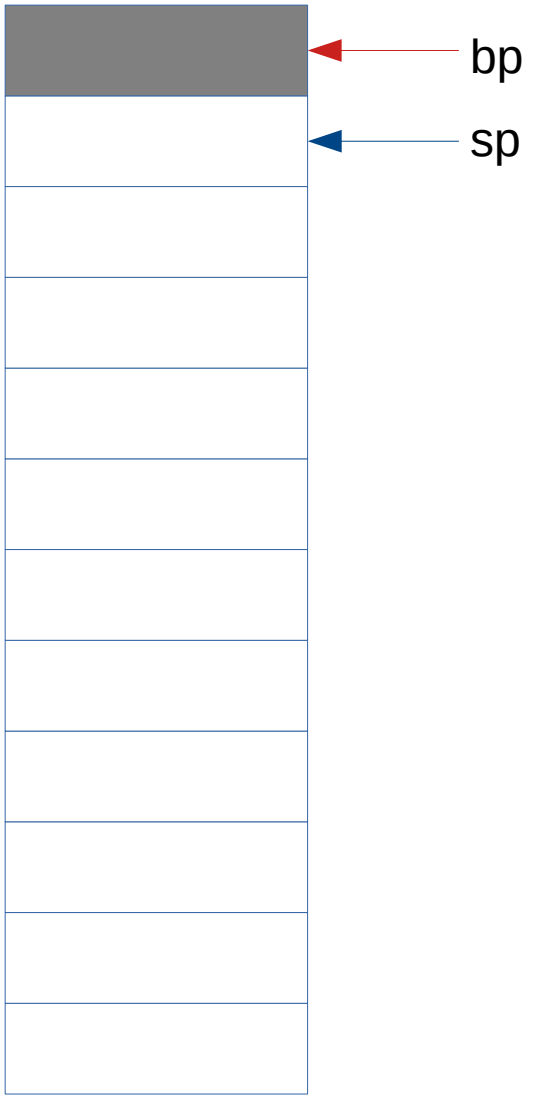

```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}



char *answer( char *question)
{
   static char buffer[20];
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

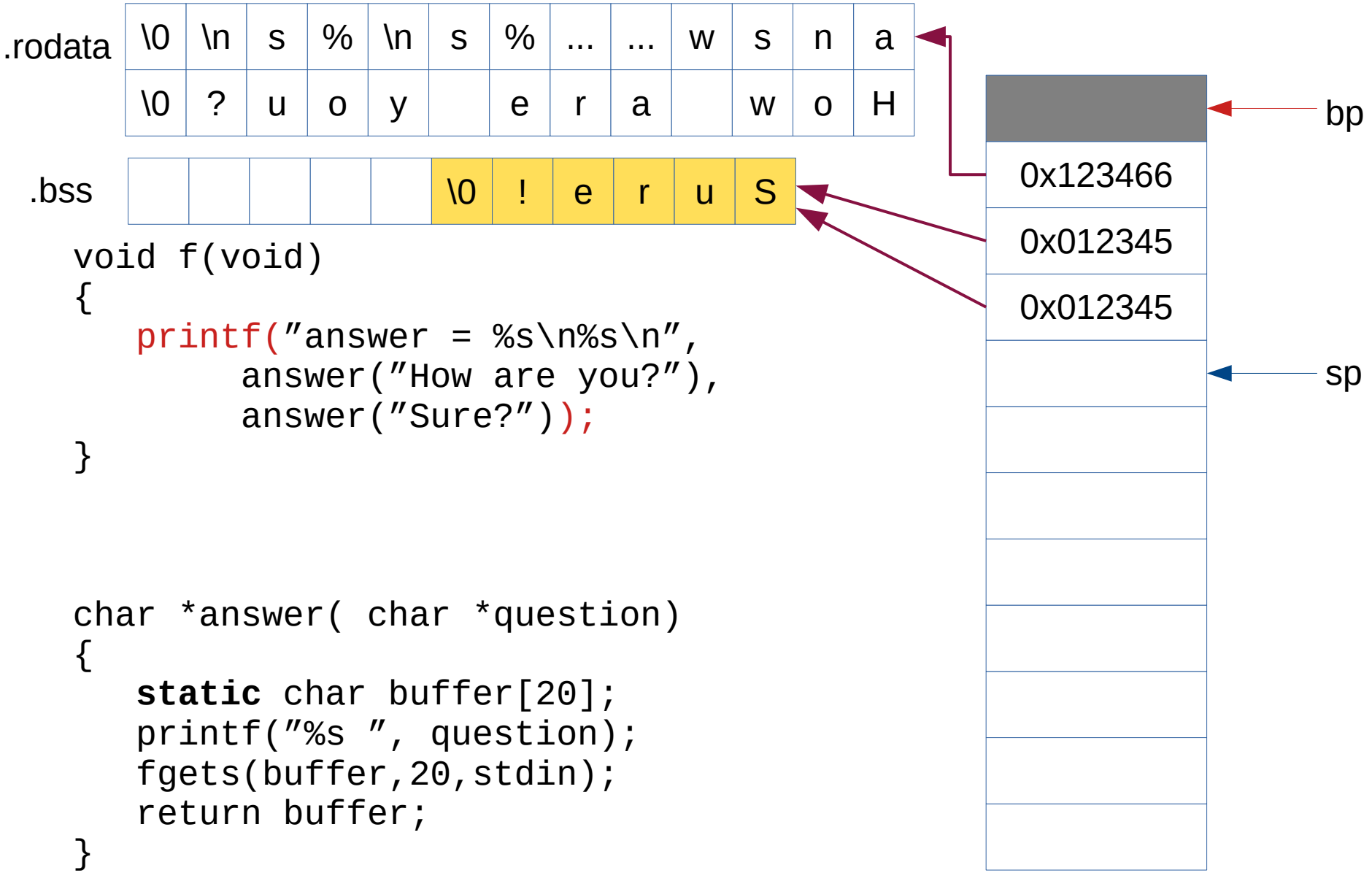



.rodata
\0 \n s % \n s % ... ... w s n a
\0 ? u o y e r a w o H
.bss
\0 ! e n i F
void f(void)
{
printf("answer = %s\n%s\n",
answer("How are you?"),
answer("Sure?"));
}
char *answer(char *question)
{
static char buffer[20];
printf("%s ", question);
fgets(buffer,20,stdin);
return buffer;
}
0x012345


bp
sp

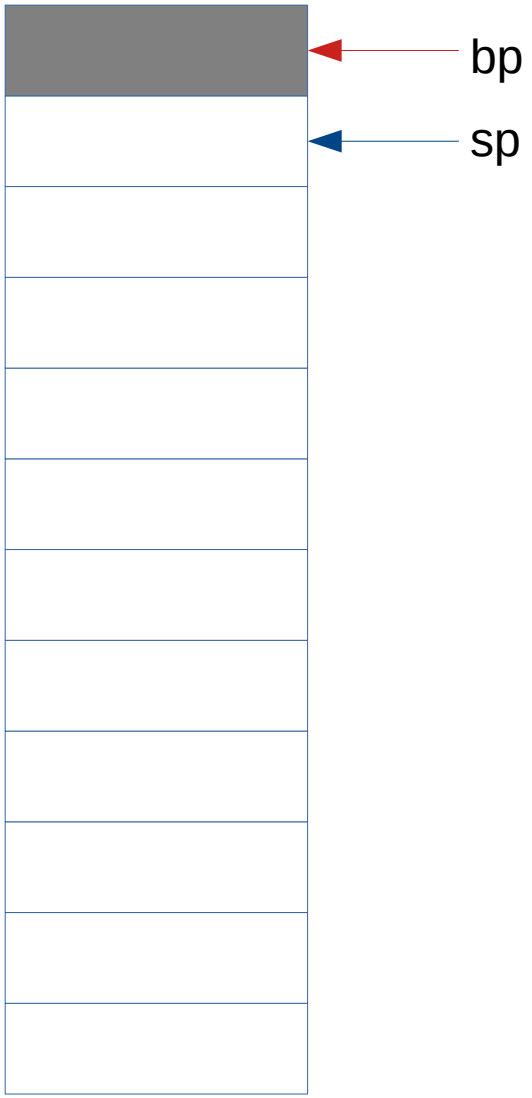

.rodata
\0 \n s % \n s % ... ... w s n a
\0 ? u o y e r a w o H
.bss
\0 ! e r u S
void f(void)
{
printf("answer = %s\n%s\n",
answer("How are you?"),
answer("Sure?"));
}
char *answer(char *question)
{
static char buffer[20];
printf("%s ", question);
fgets(buffer,20,stdin);
return buffer;
}
0x012345


bp
sp

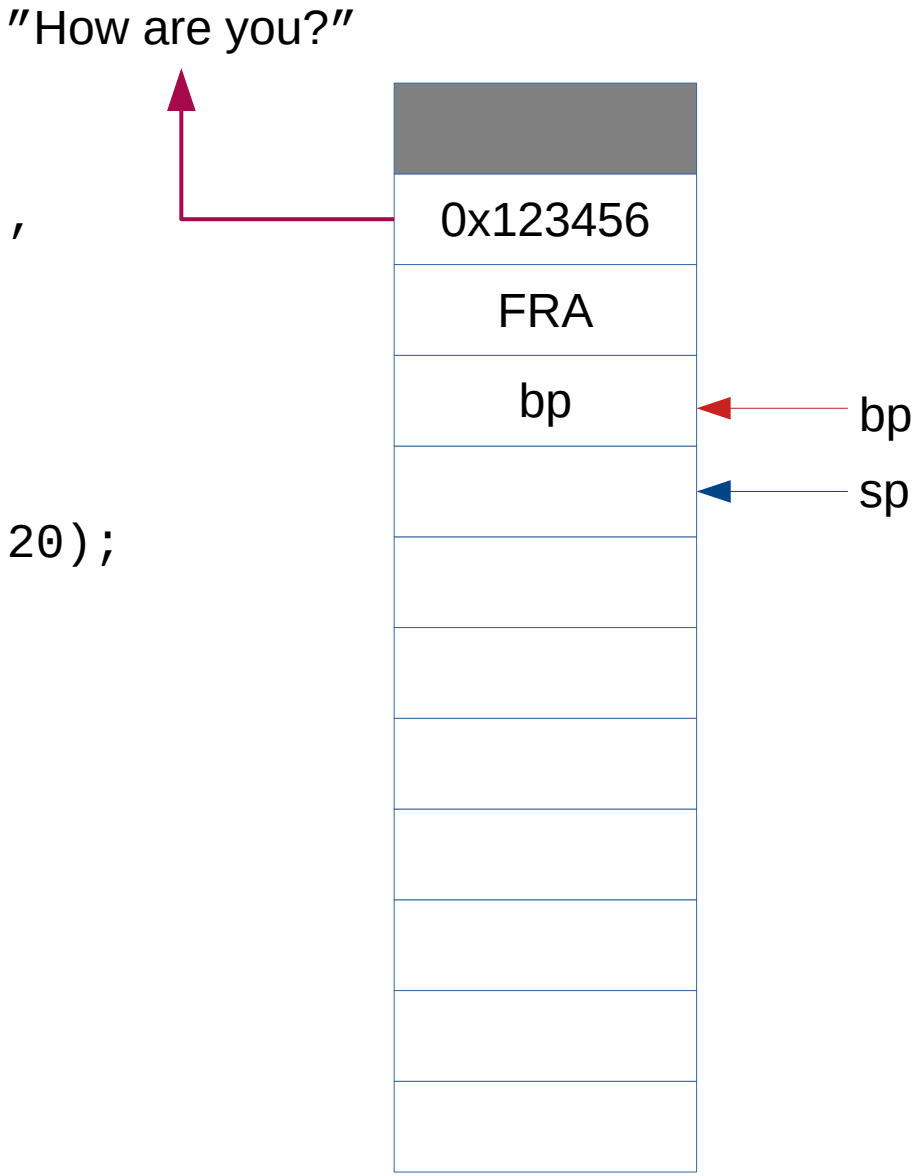



```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}



char *answer( char *question)
{
   static char buffer[20];
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

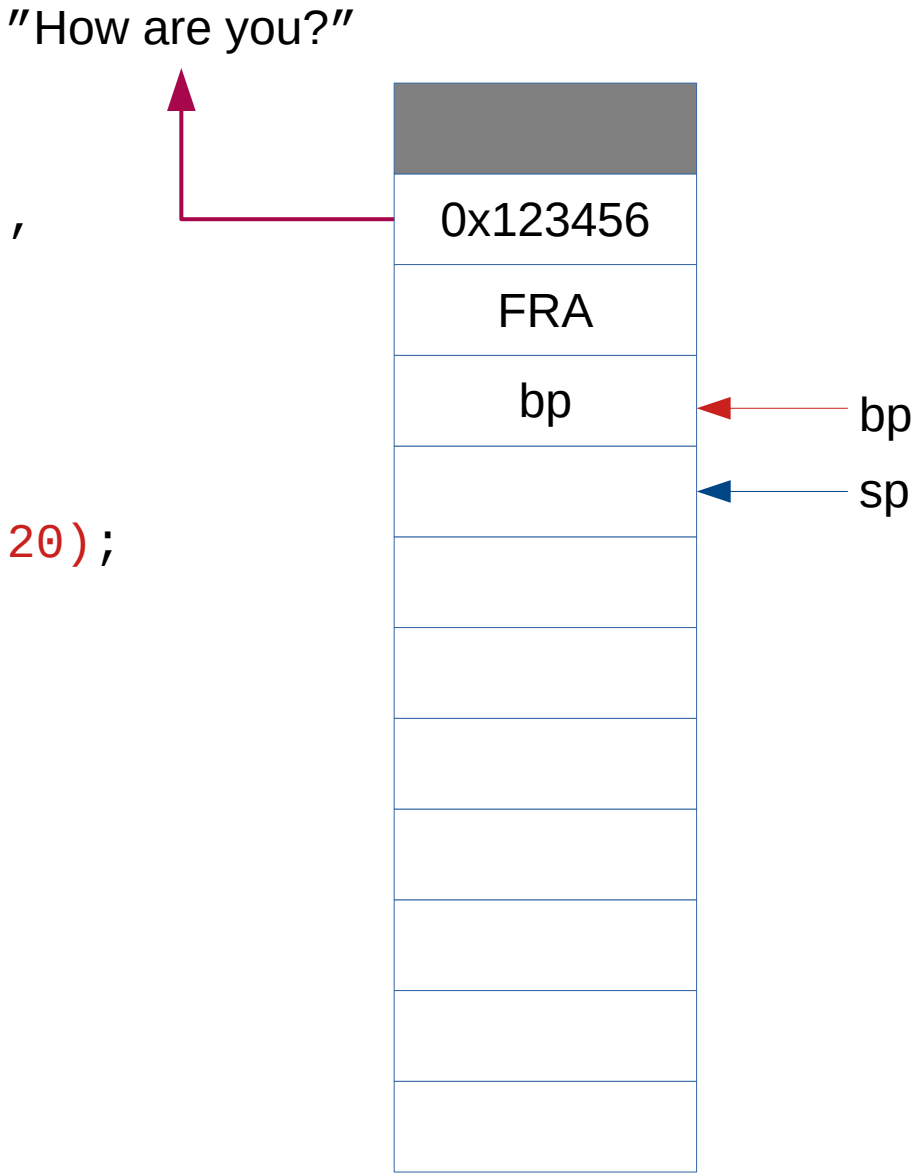
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



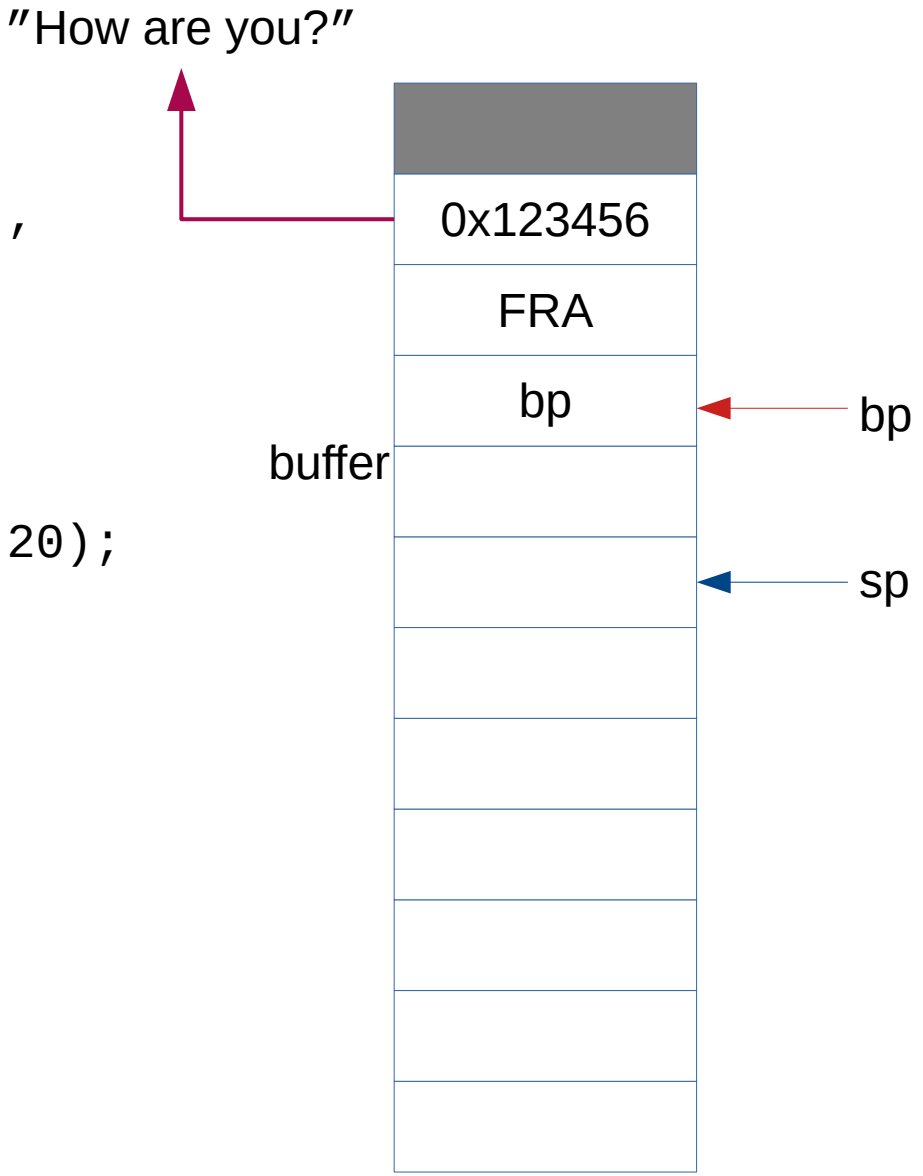
```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
      return "No memory";
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



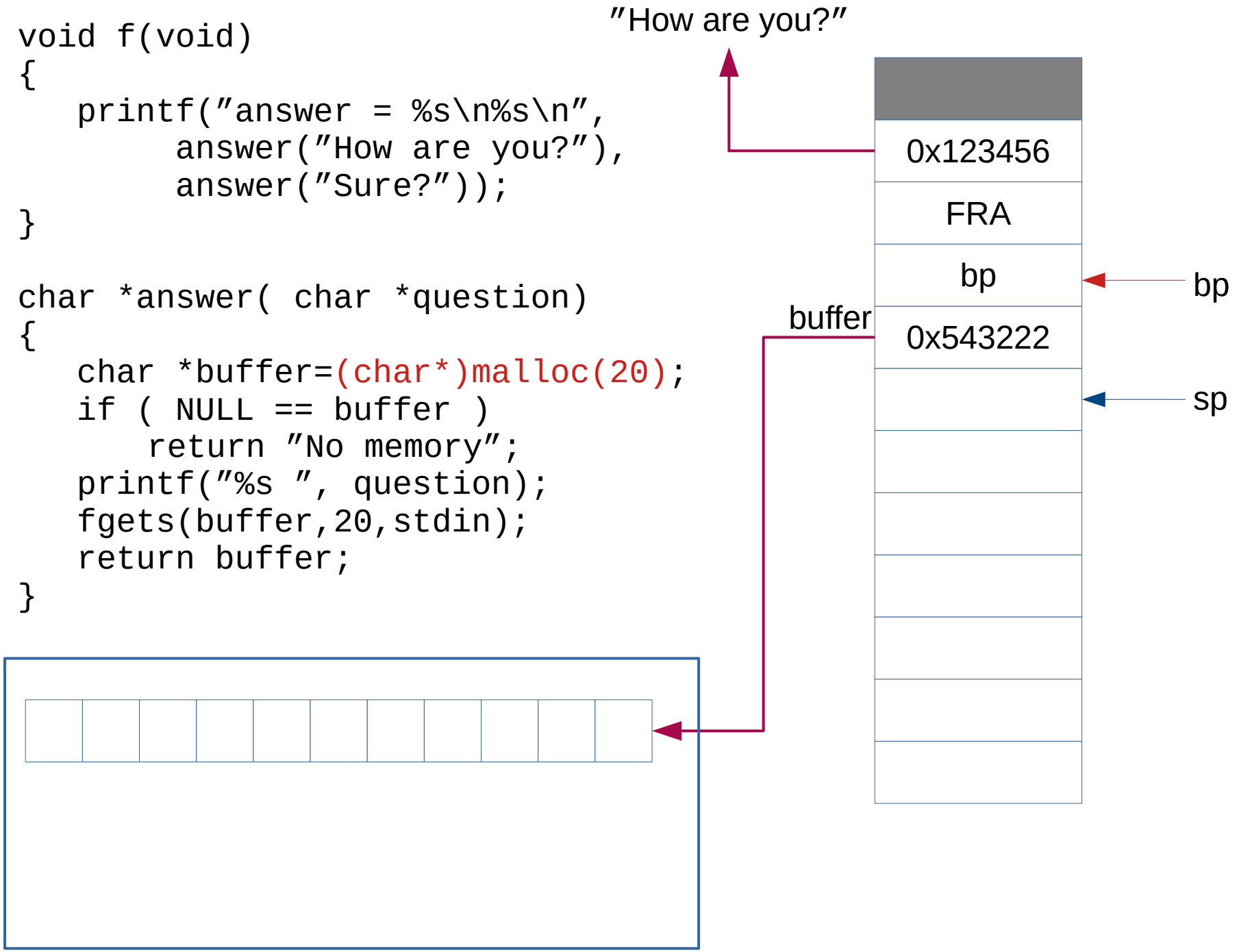
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



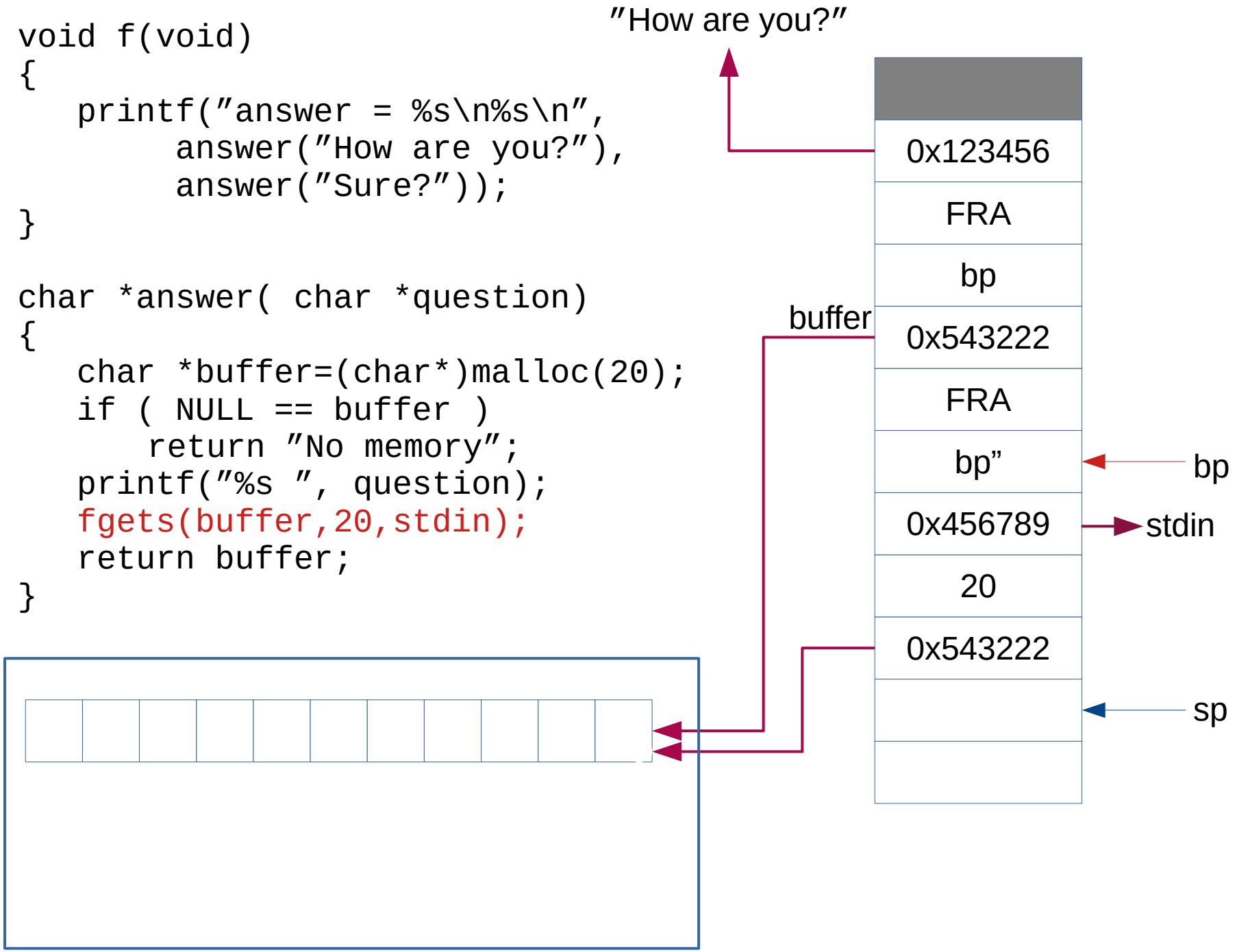
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



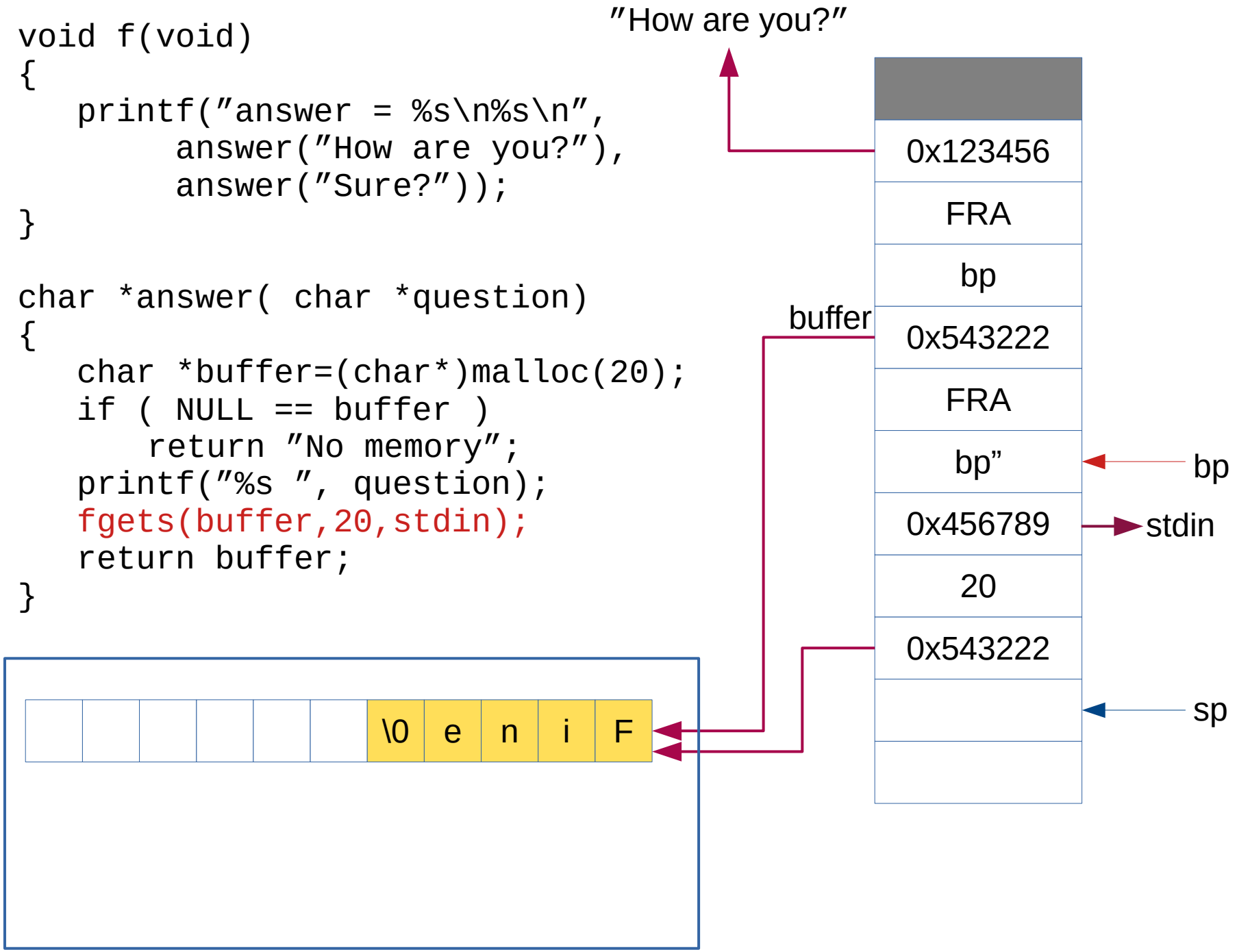
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



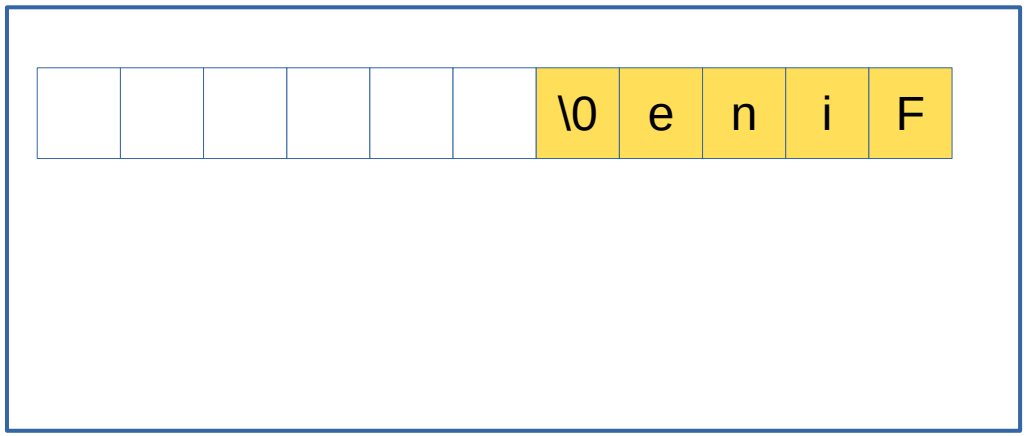
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

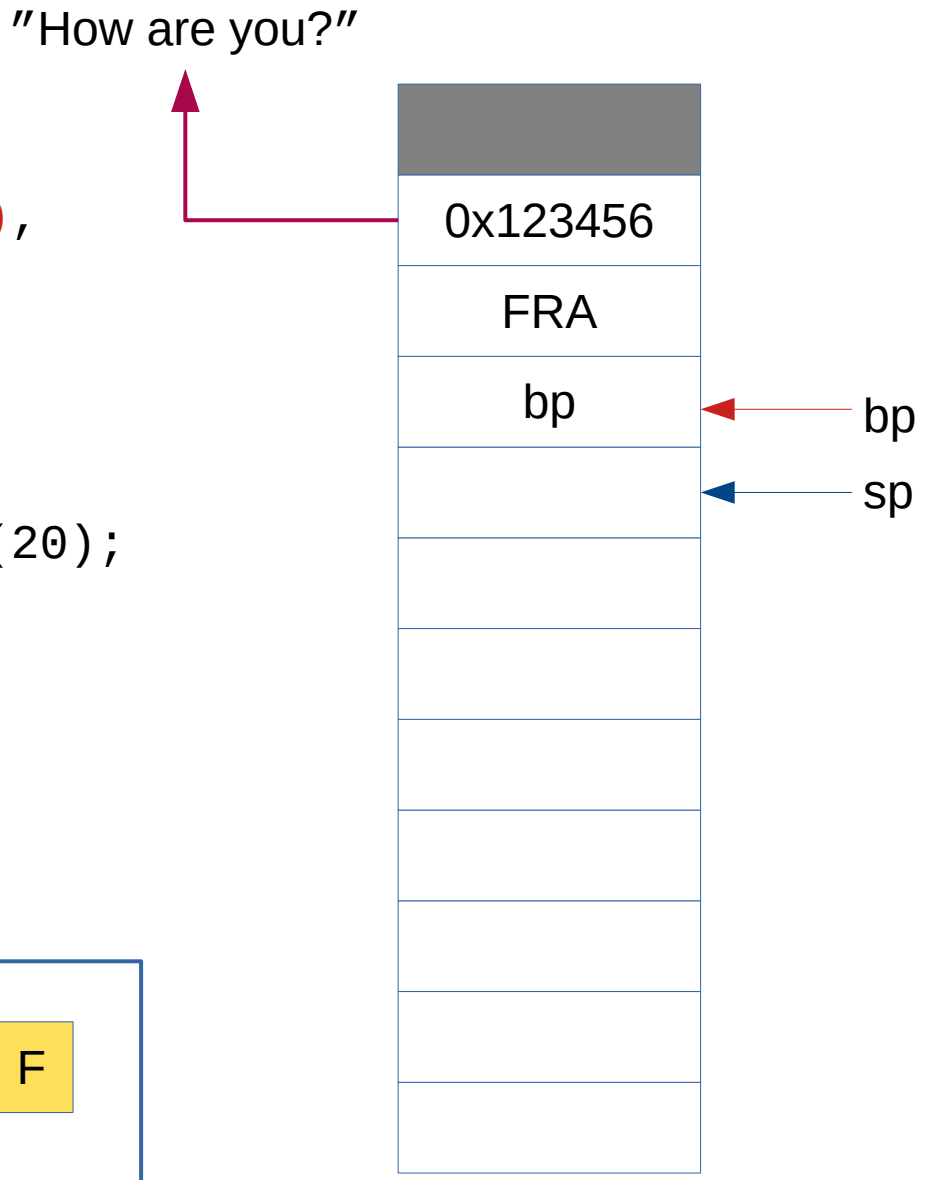


```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

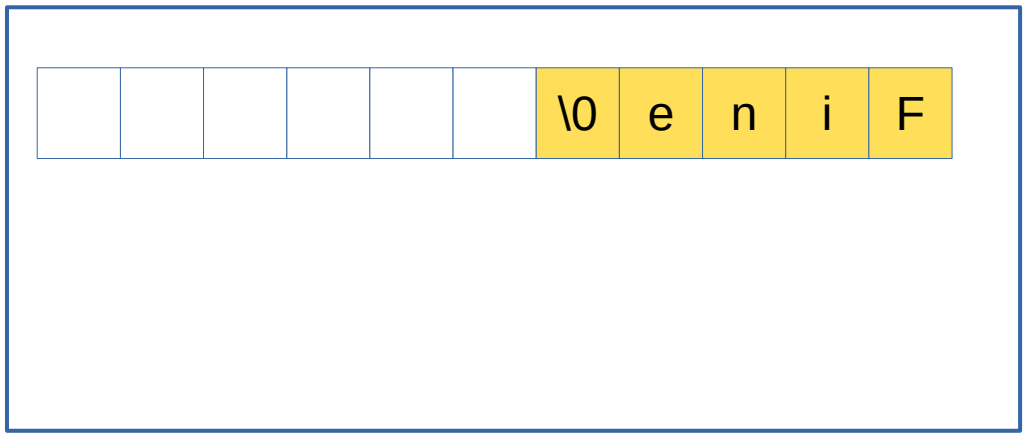


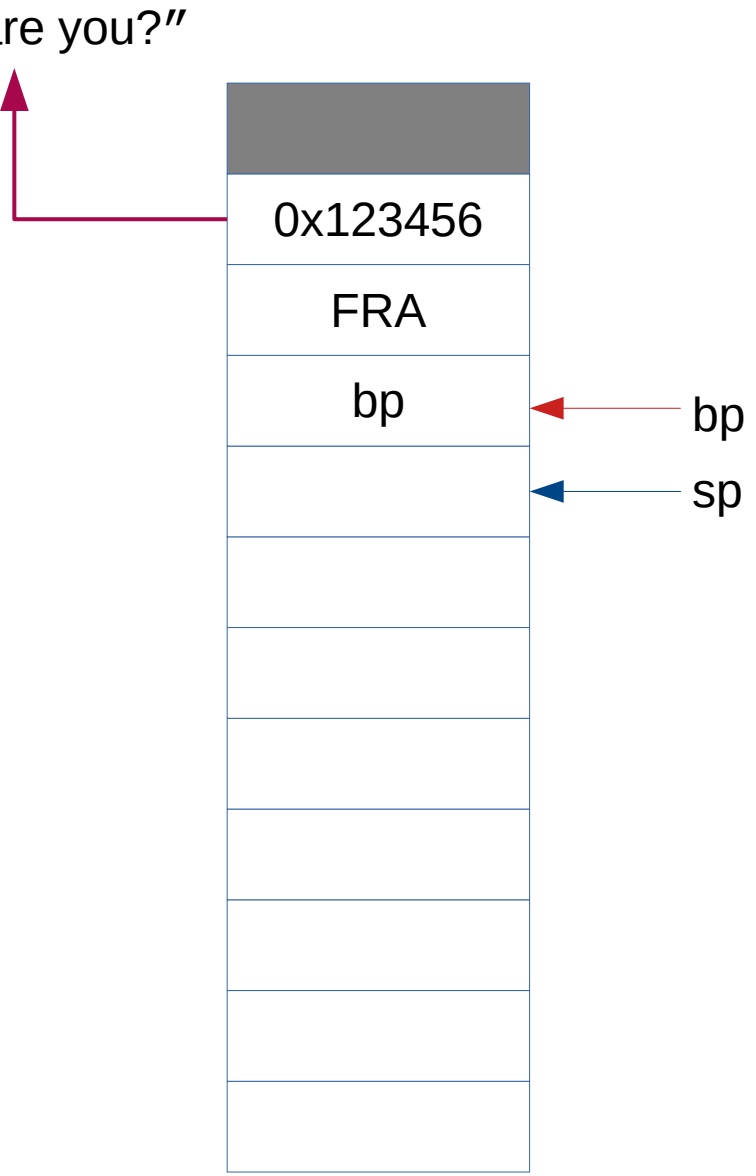
```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
      return "No memory";
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



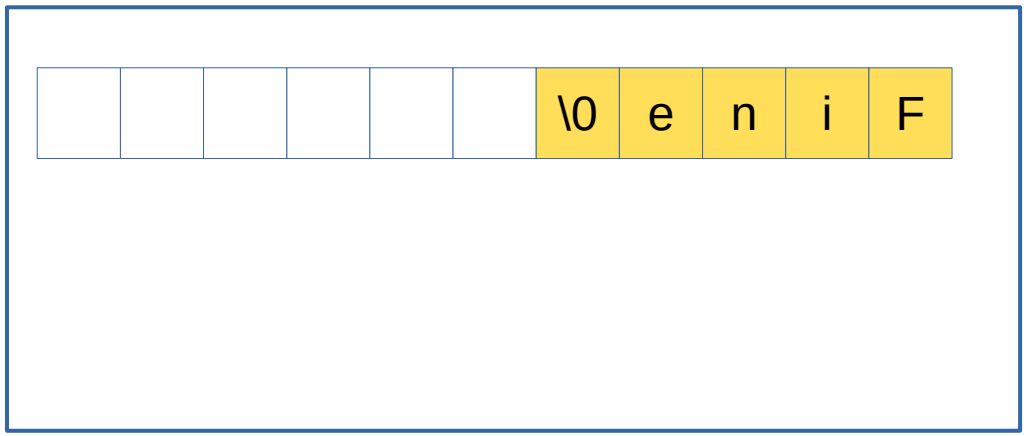


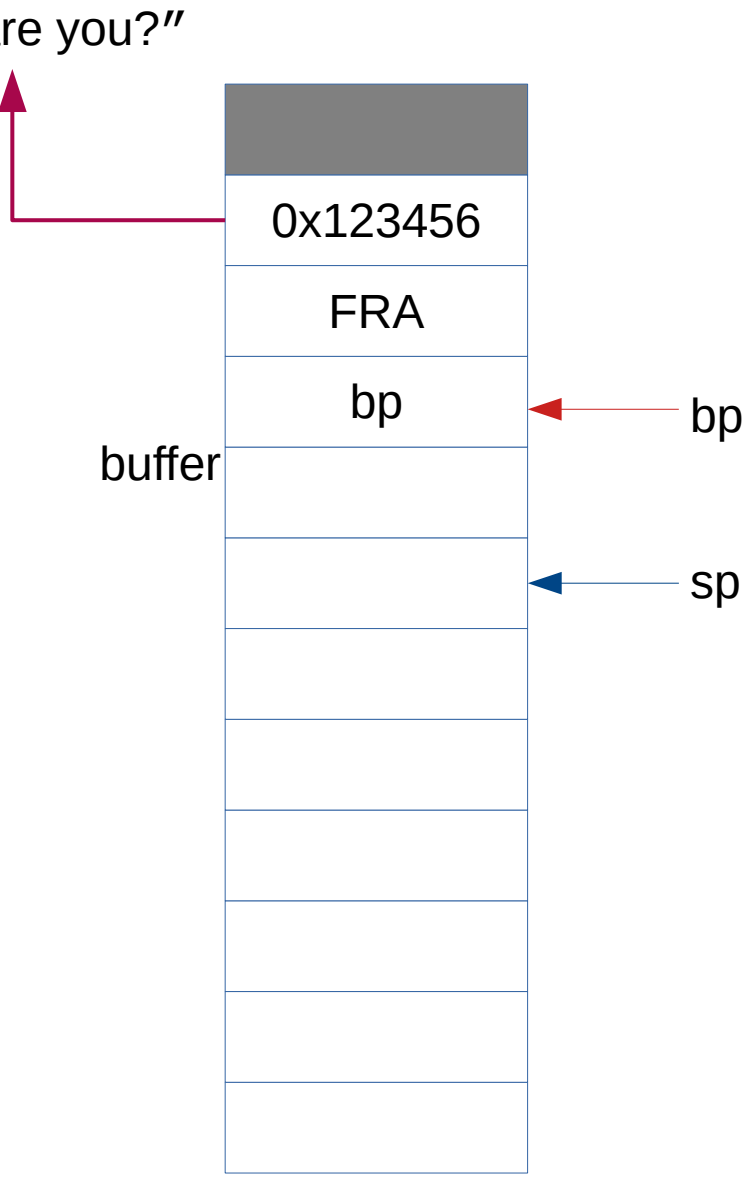
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



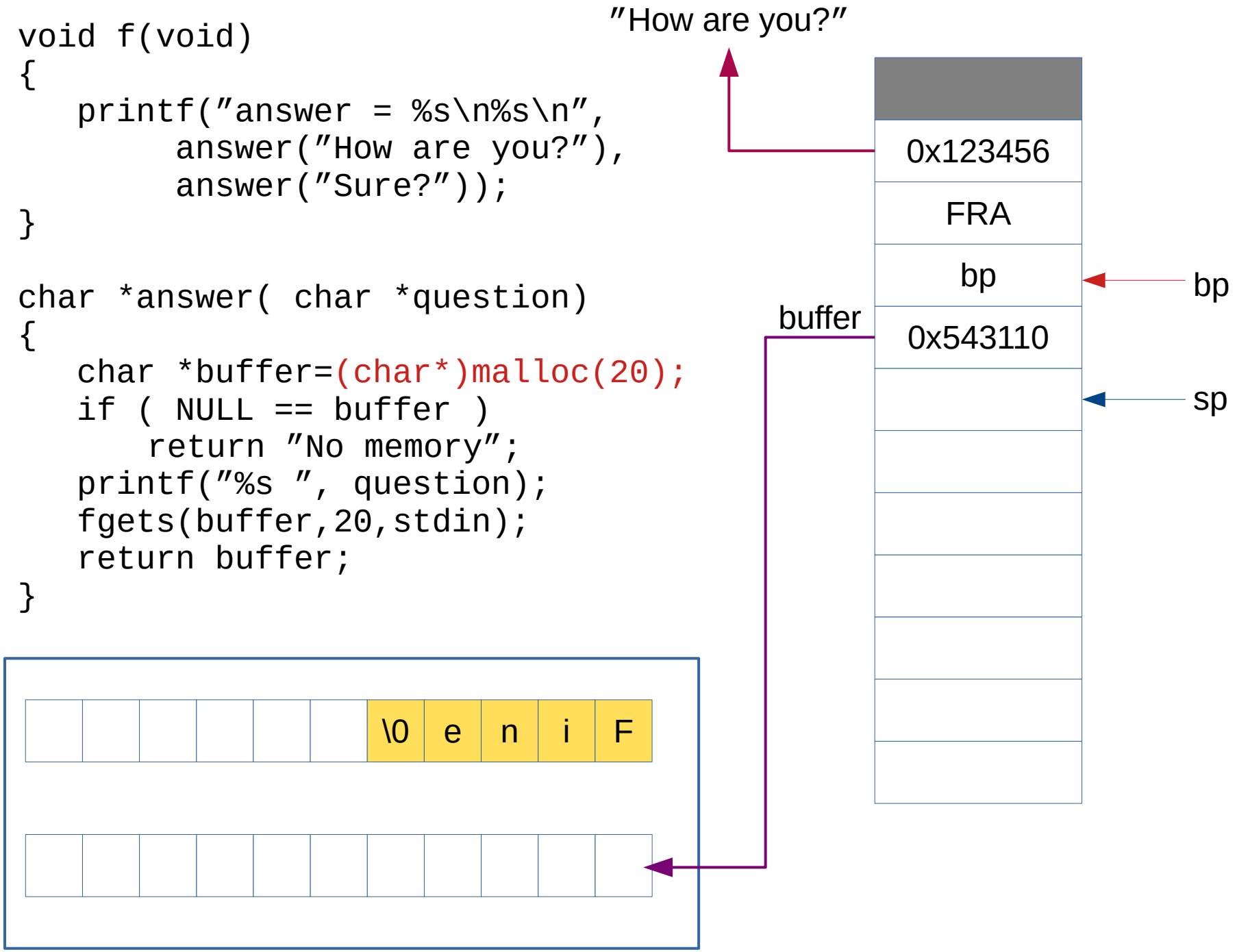


```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

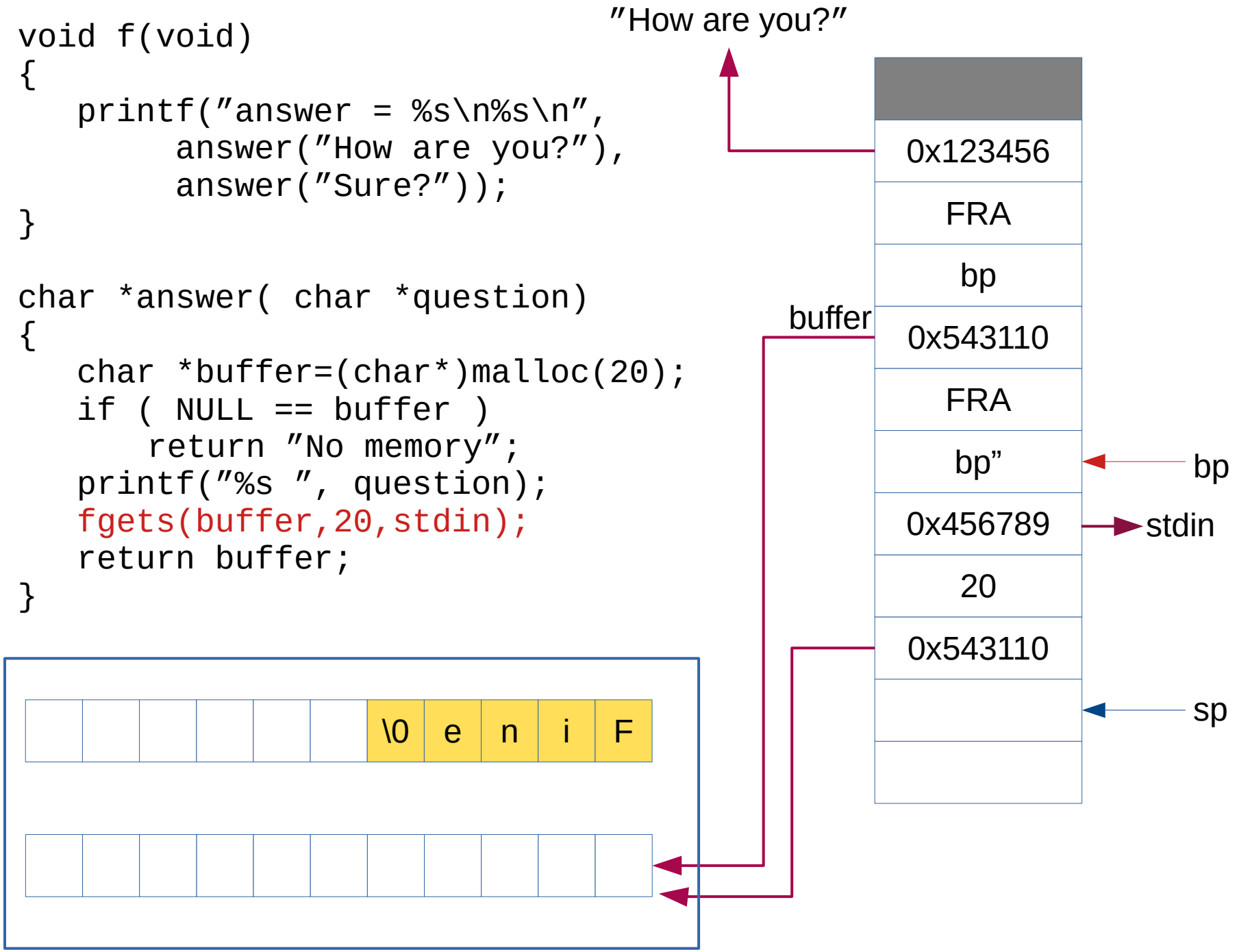




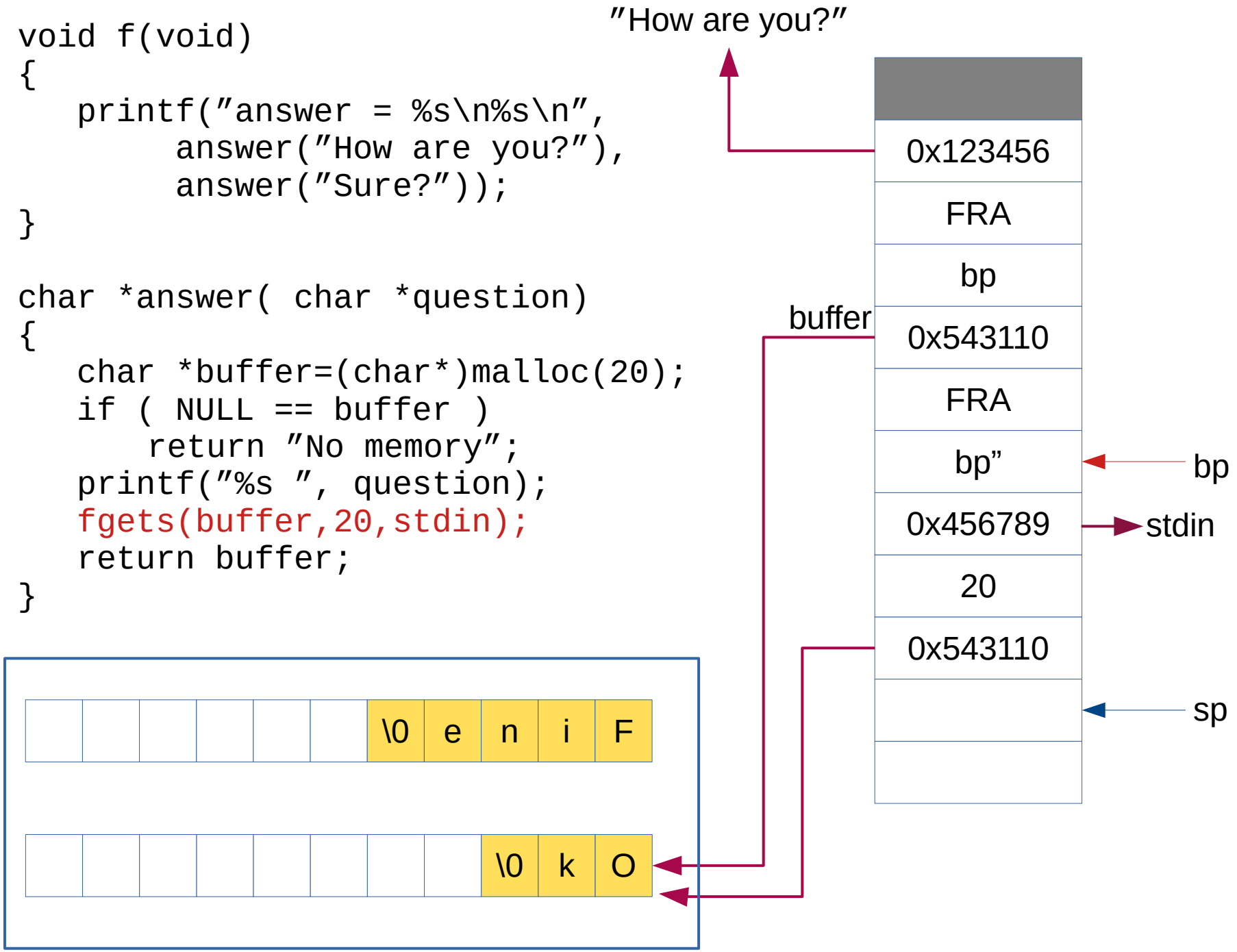
```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return "No memory";
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



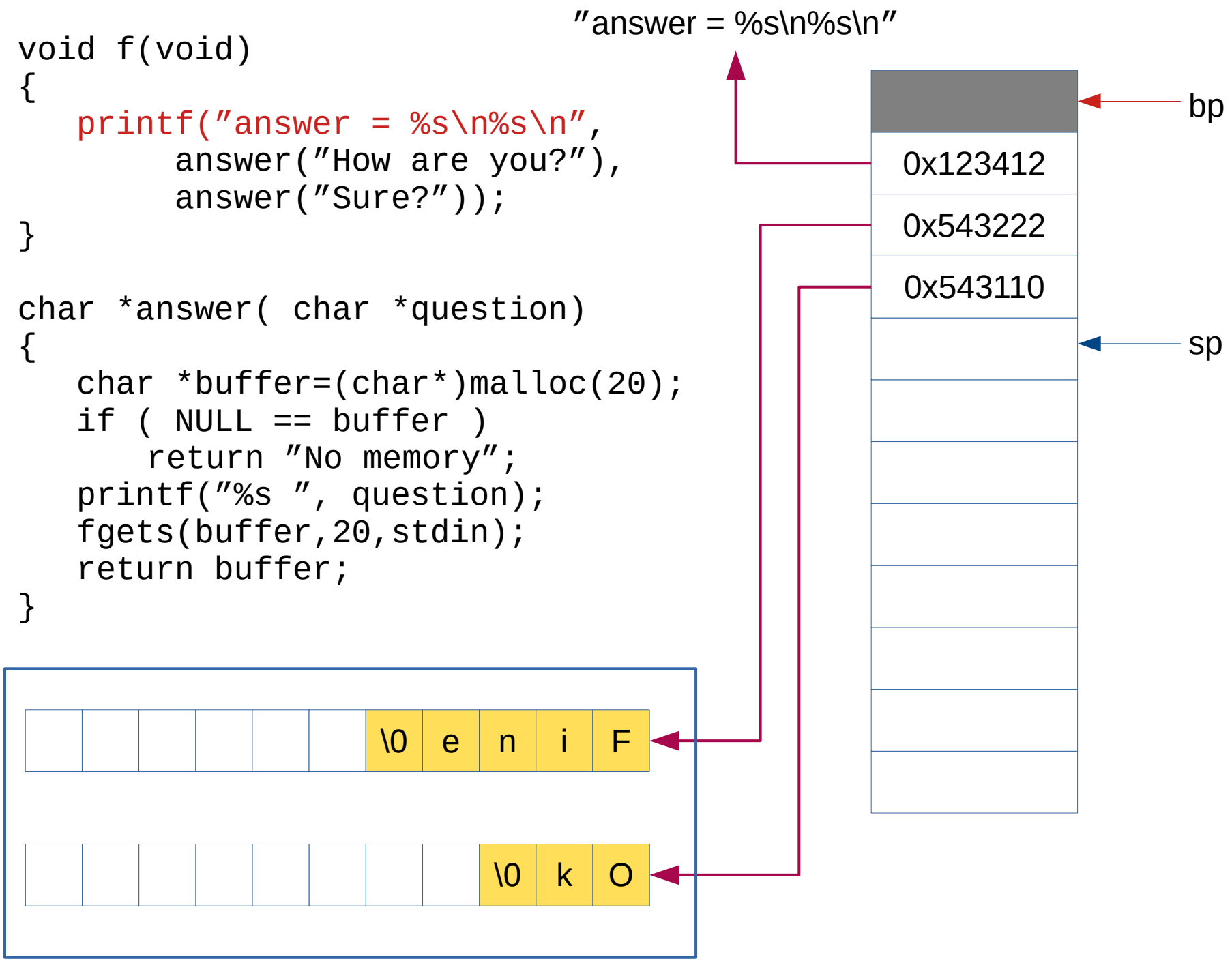
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



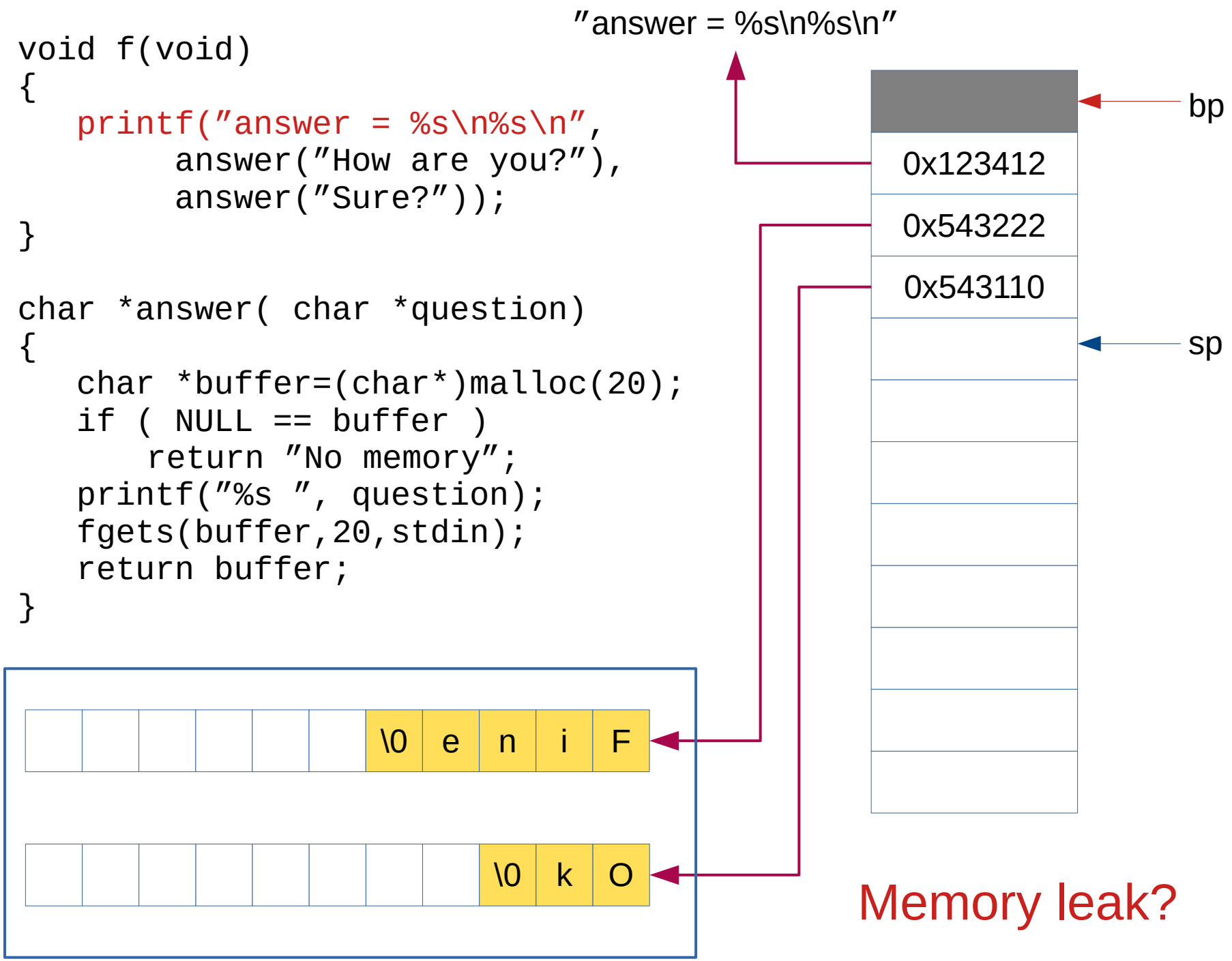
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



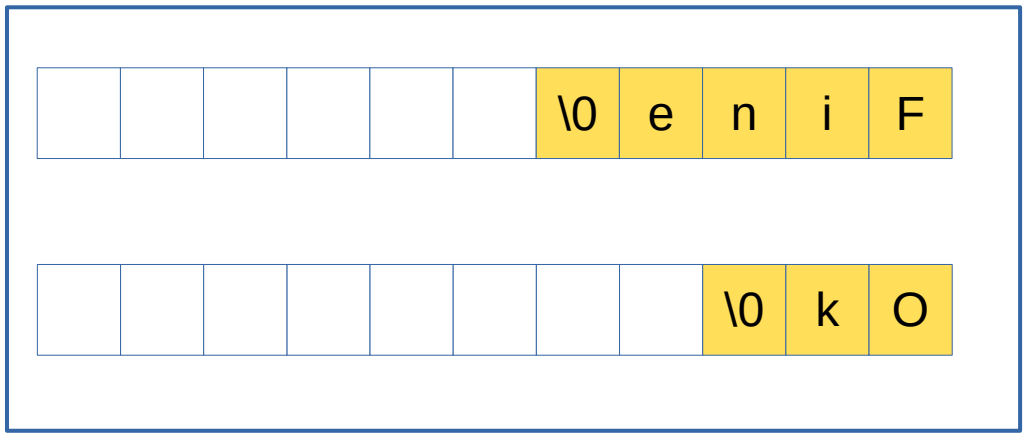
```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return "No memory";
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```

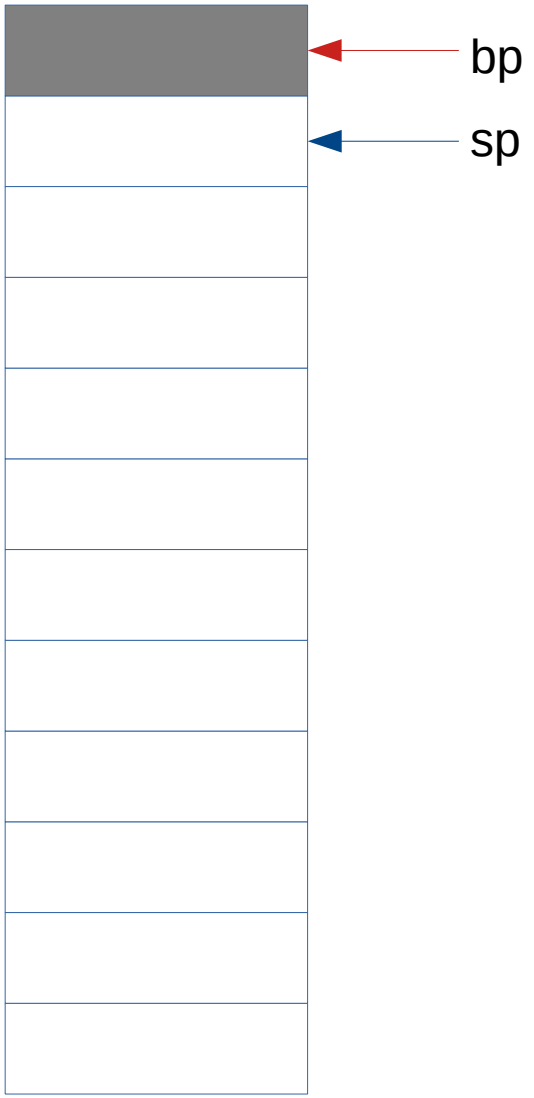


```
void f(void)
{
   printf("answer = %s\n%s\n",
        answer("How are you?"),
        answer("Sure?"));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return "No memory";
   printf("%s ", question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



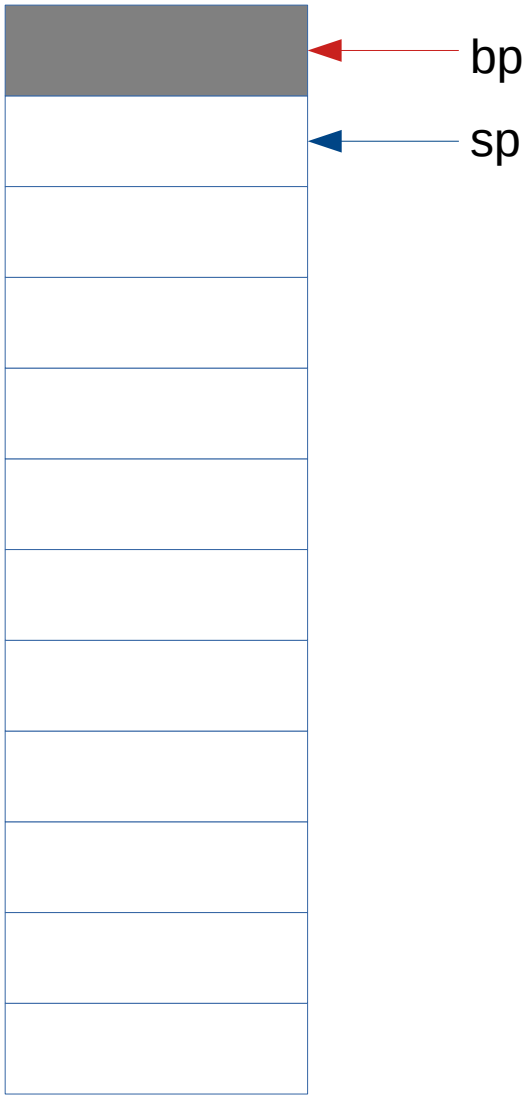
```
void f(void)
{
   printf(”answer = %s\n%s\n”,
        answer(”How are you?”),
        answer(”Sure?”));
}

char *answer( char *question)
{
   char *buffer=(char*)malloc(20);
   if ( NULL == buffer )
       return ”No memory”;
   printf(”%s ”, question);
   fgets(buffer,20,stdin);
   return buffer;
}
```



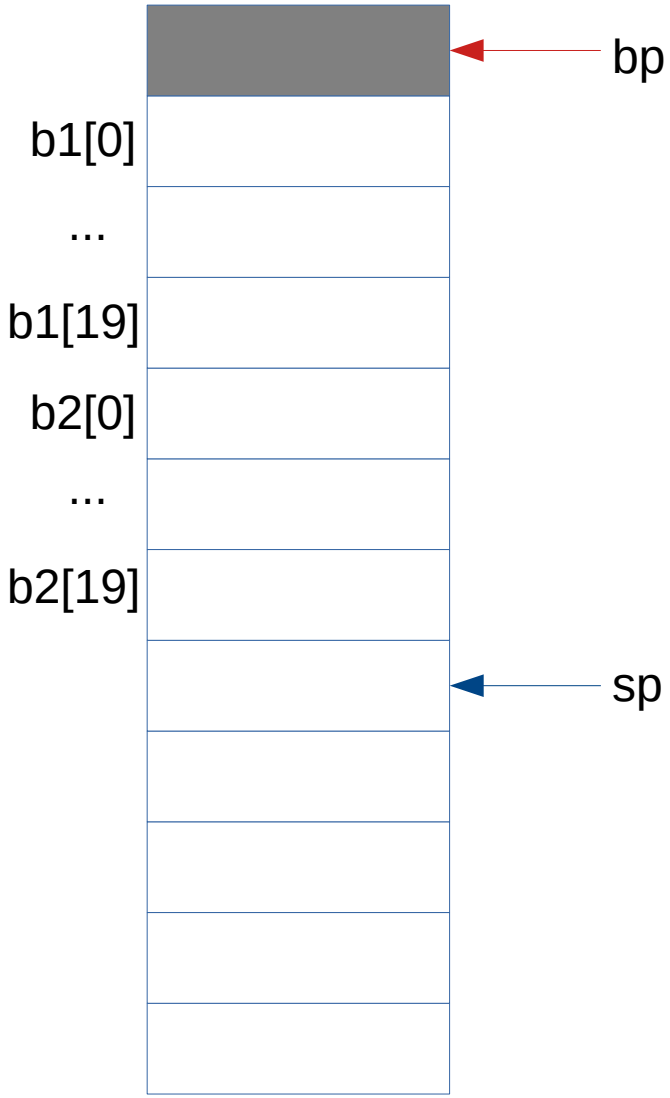


Memory leak?

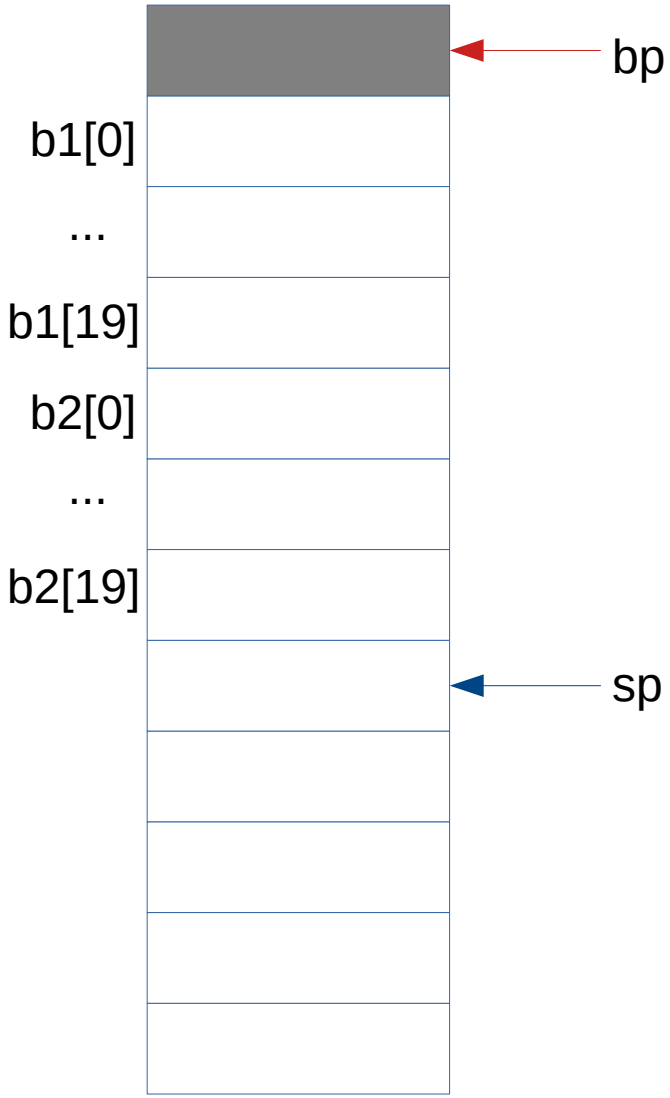
```
void f(void)
{
   char b1[20];
   char b2[20];

    printf(”answer = %s\n%s\n”,
        answer(”How are you?”,b1,20),
        answer(”Sure?”, b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf(”%s ”, question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



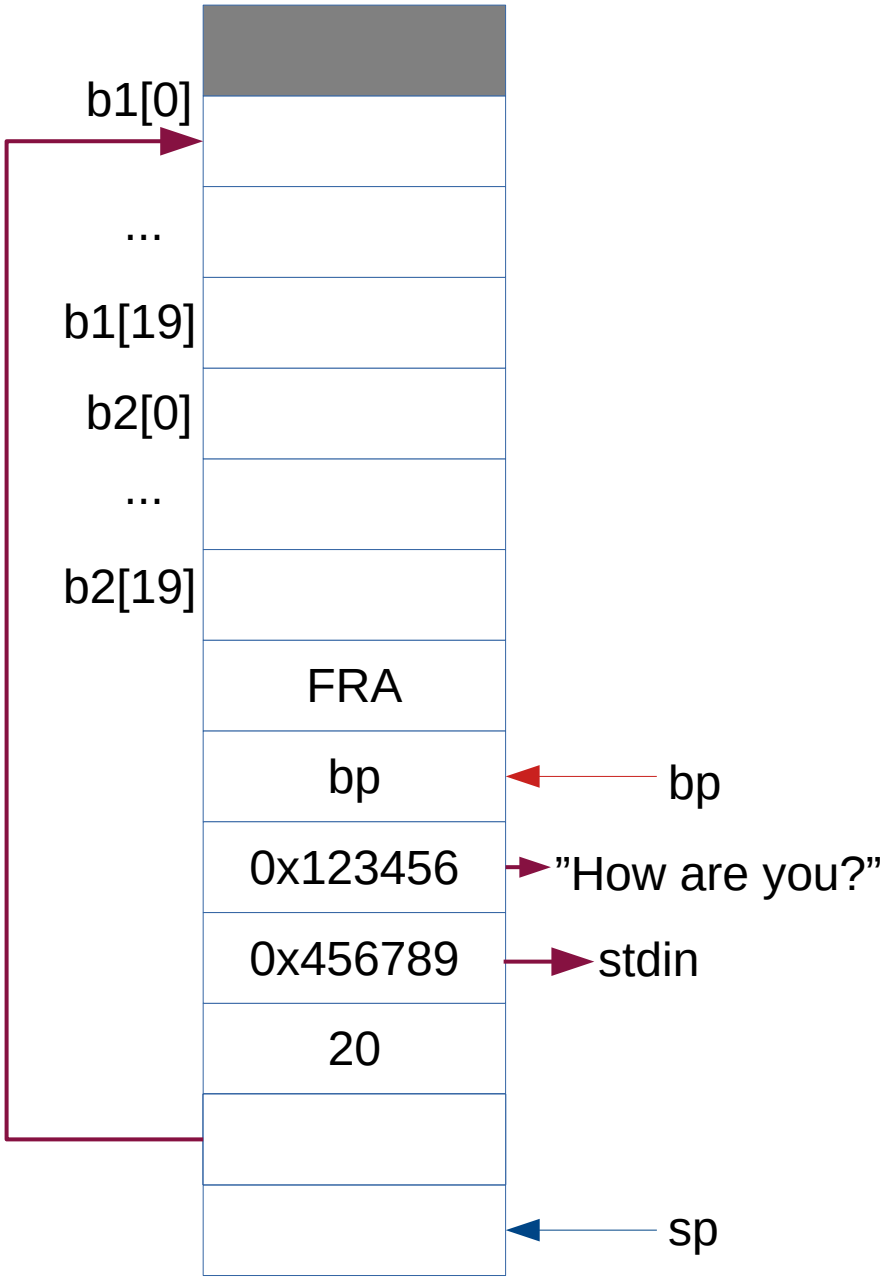
```
void f(void)
{
   char b1[20];
   char b2[20];

    printf(”answer = %s\n%s\n”,
        answer(”How are you?”,b1,20),
        answer(”Sure?”, b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf(”%s ”, question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



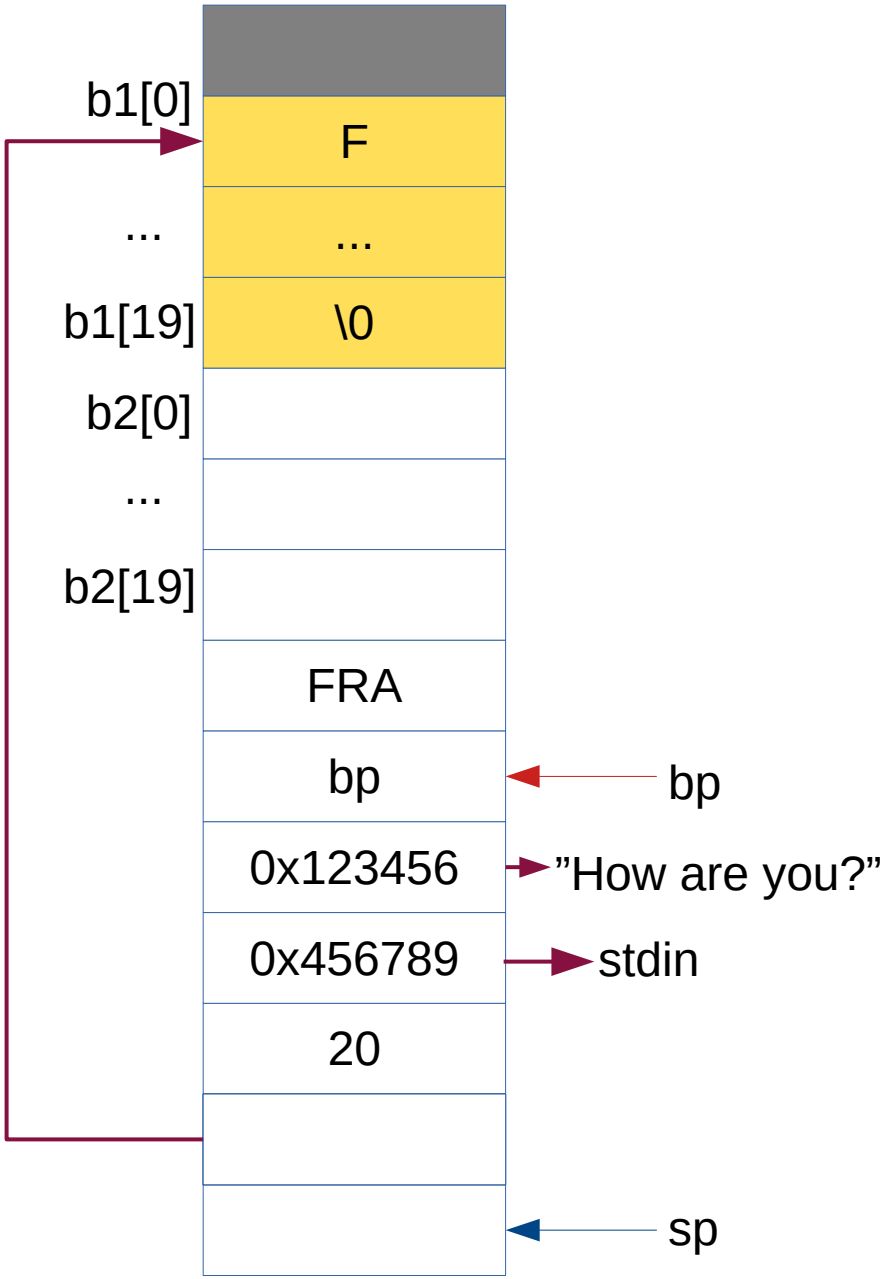
```
void f(void)
{
   char b1[20];
   char b2[20];

    printf(”answer = %s\n%s\n”,
        answer(”How are you?”,b1,20),
        answer(”Sure?”, b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf(”%s ”, question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



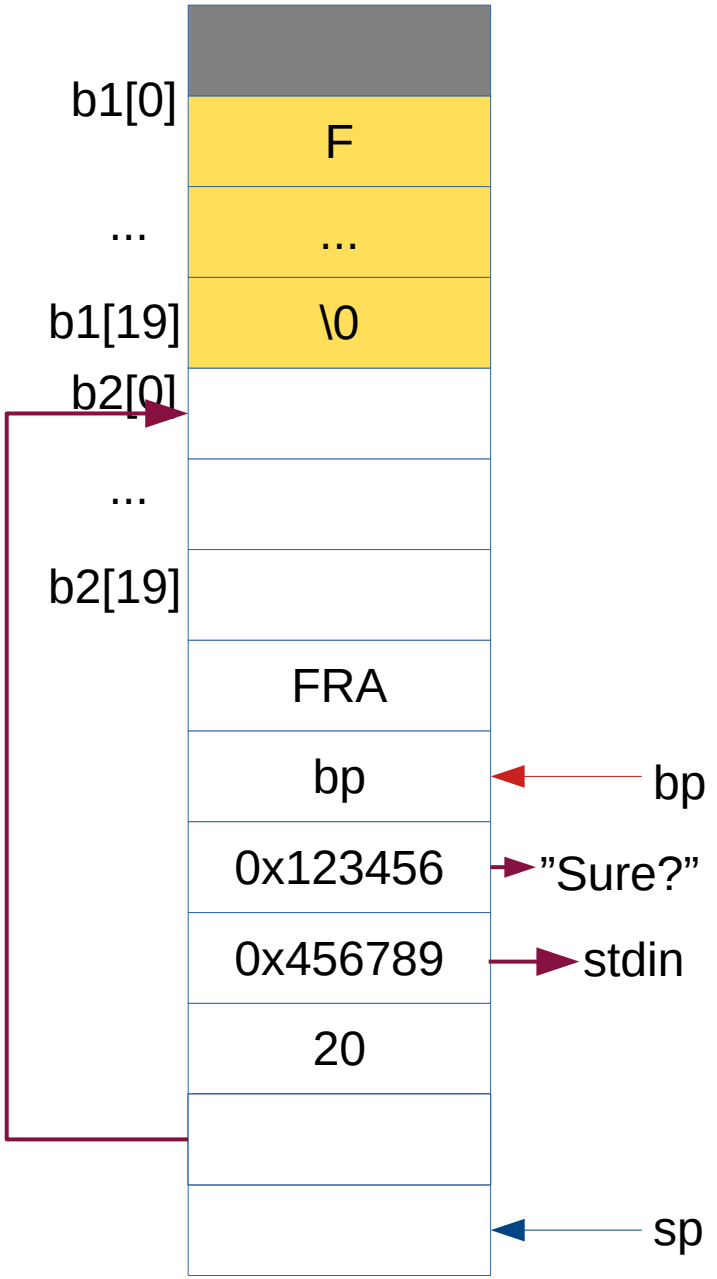
```
void f(void)
{
   char b1[20];
   char b2[20];

   printf("answer = %s\n%s\n",
       answer("How are you?",b1,20),
       answer("Sure?", b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf("%s ", question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



```
void f(void)
{
   char b1[20];
   char b2[20];

    printf("answer = %s\n%s\n",
        answer("How are you?",b1,20),
        answer("Sure?", b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf("%s ", question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



```
void f(void)
{
   char b1[20];
   char b2[20];

    printf("answer = %s\n%s\n",
        answer("How are you?",b1,20),
        answer("Sure?", b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf("%s ", question);
   fgets(buffer,len,stdin);
   return buffer;
}
```



```
void f(void)
{
   char b1[20];
   char b2[20];

    printf("answer = %s\n%s\n",
        answer("How are you?",b1,20),
        answer("Sure?", b2, 20));
}

char *answer( char *question,
              char *buffer, int len)
{
   printf("%s ", question);
   fgets(buffer,len,stdin);
   return buffer;
}
```