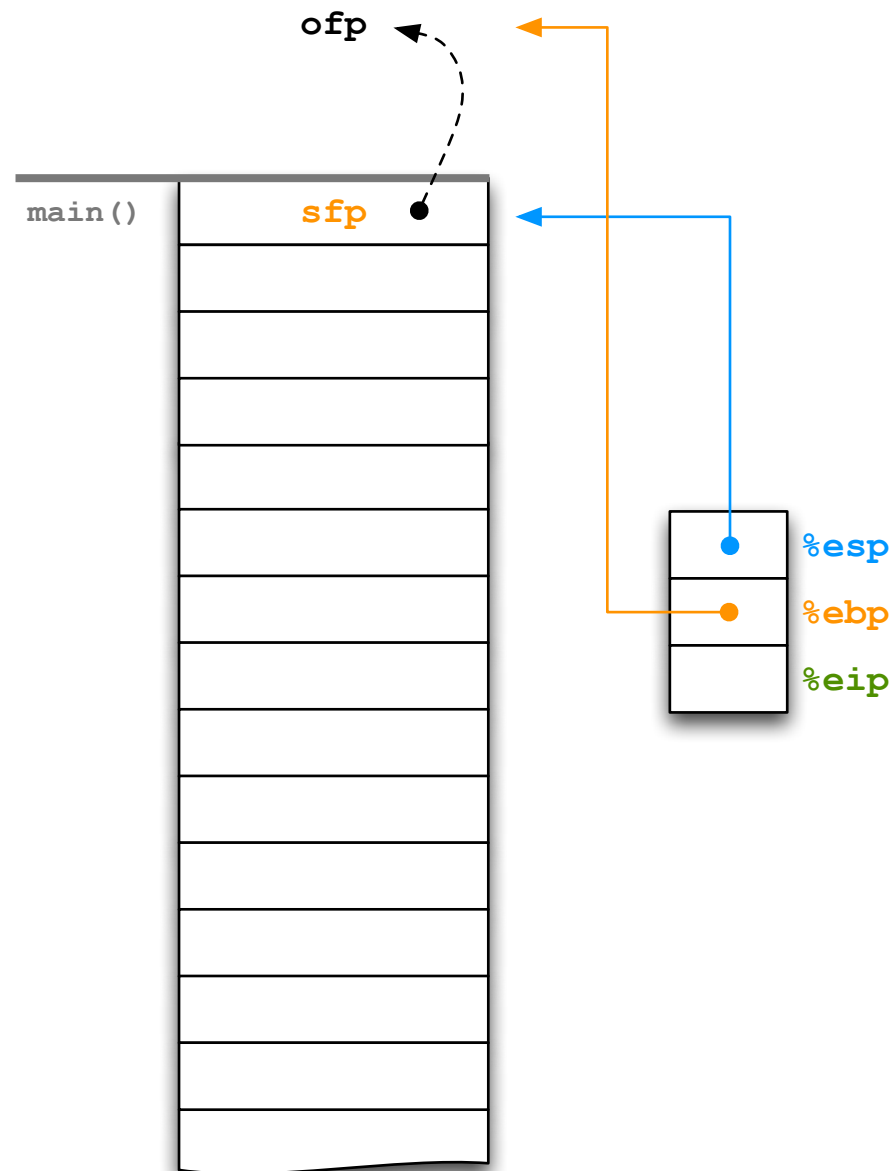```c
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs

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;
}
```

ofp

main()    sfp

%esp

%ebp
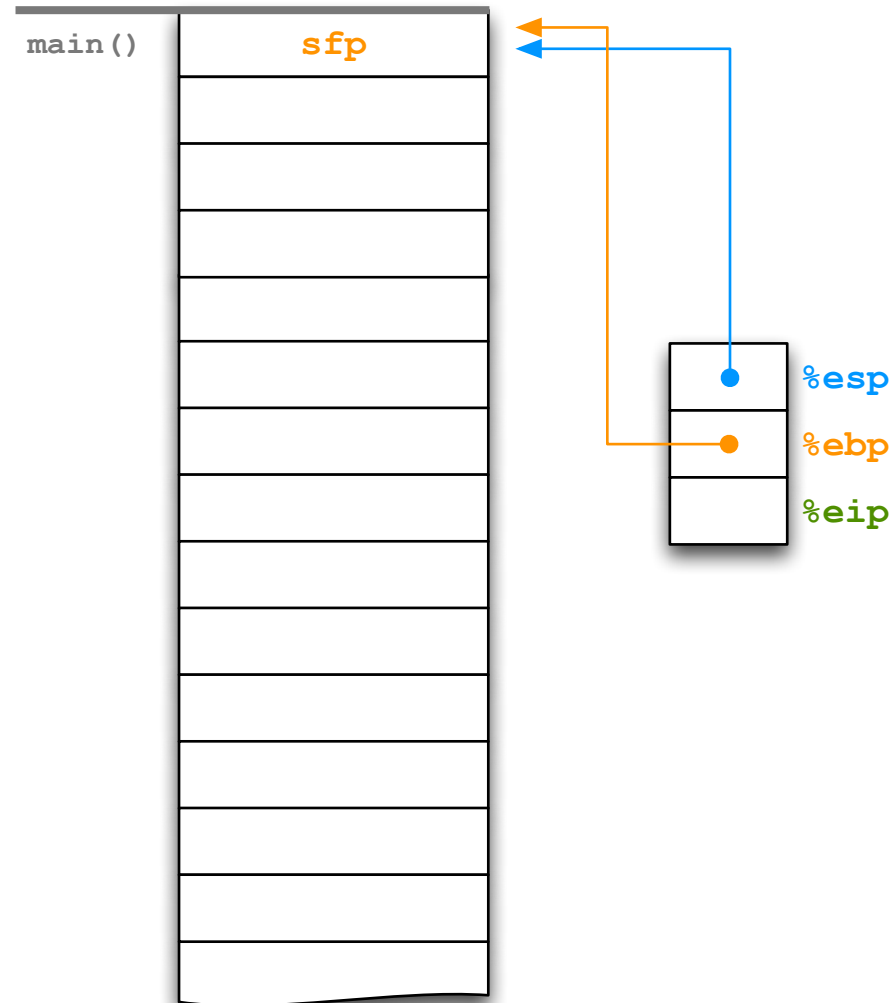
%eip

```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

%esp
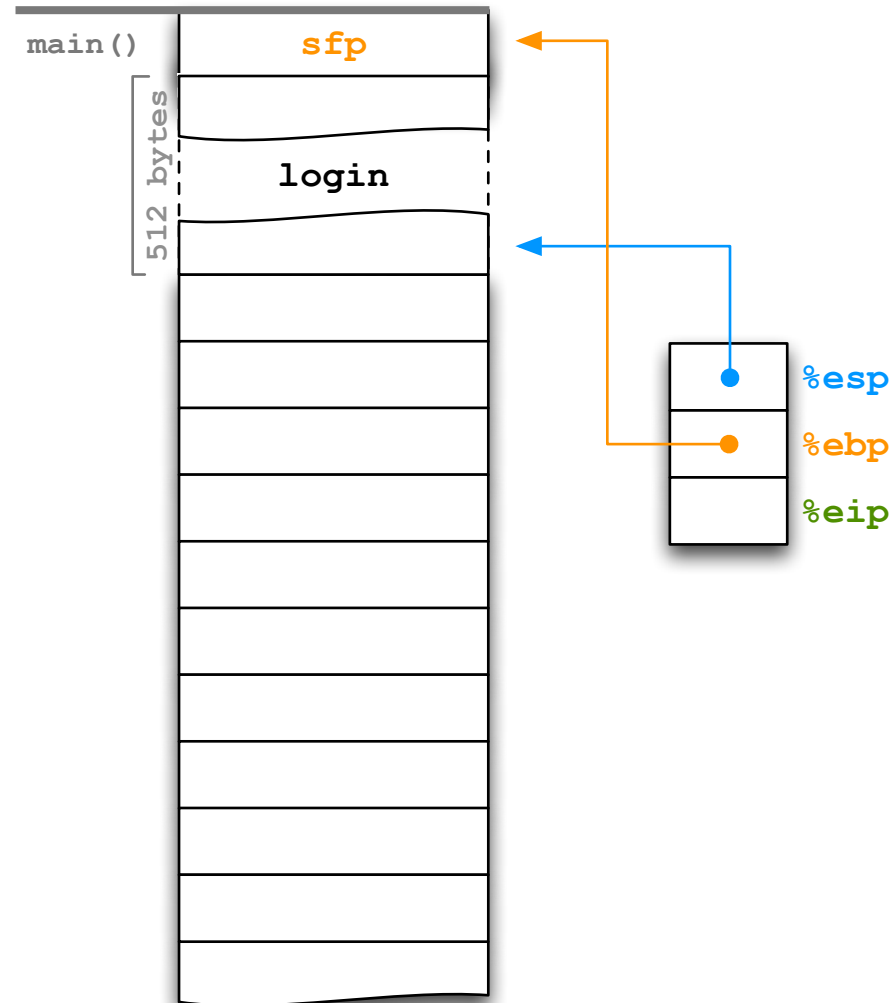%ebp
%eip

```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

512 bytes

login

%esp

%ebp
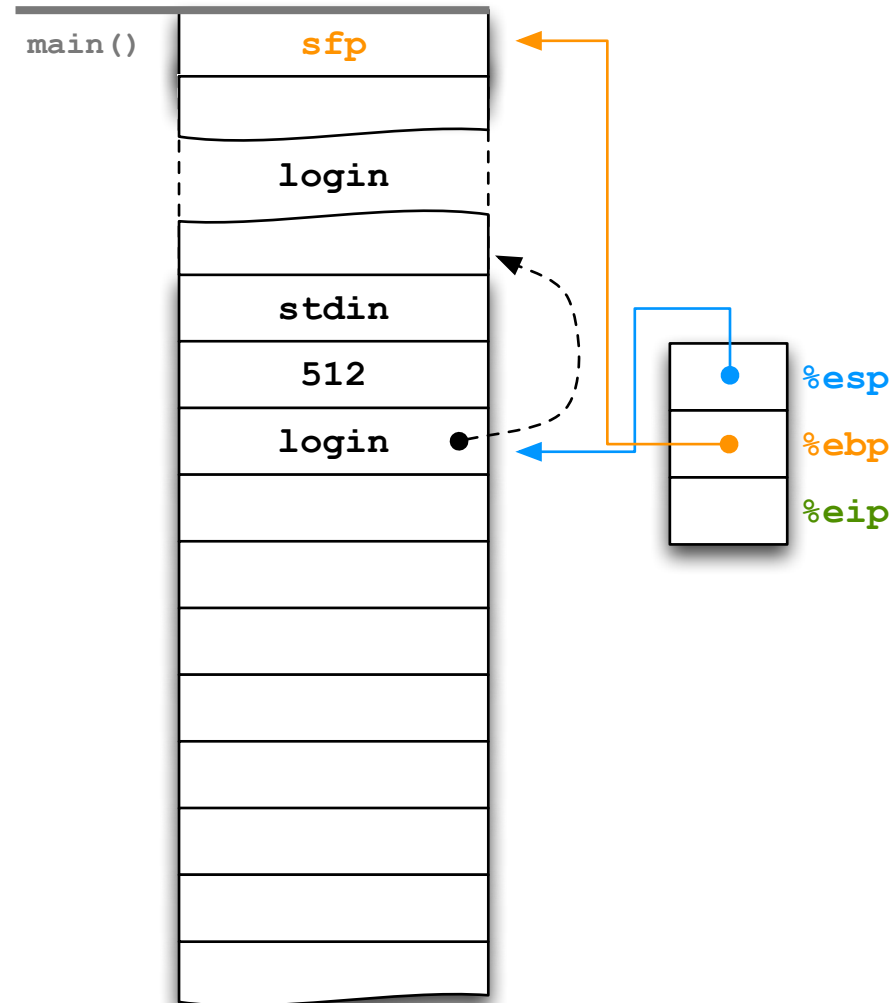
%eip

```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
stdin
512
login

%esp

%ebp
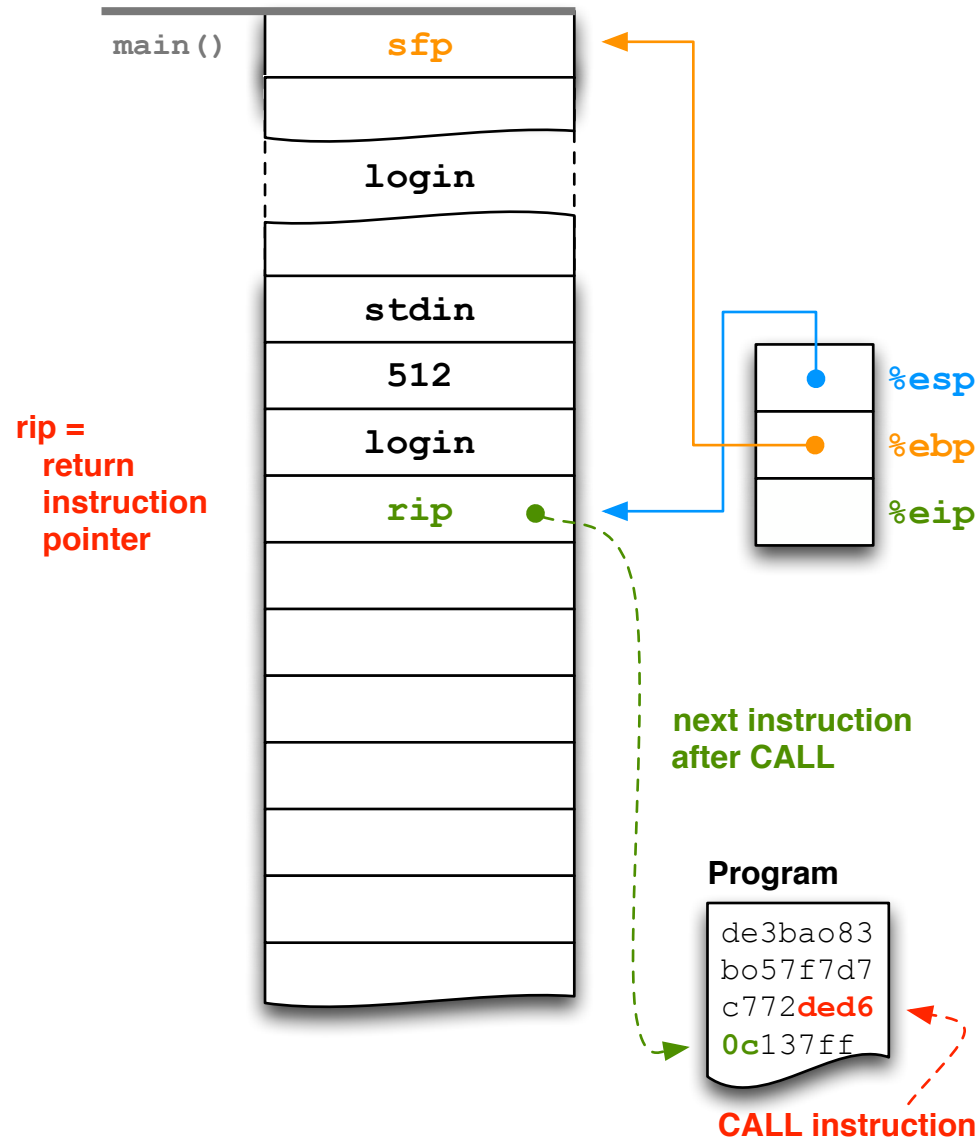
%eip

```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

stdin

512

login

rip

rip =
return
instruction
pointer

%esp

%ebp

%eip

next instruction
after CALL

Program

```
de3ba o83
bo57f7d7
c772ded6
0c137ff
```

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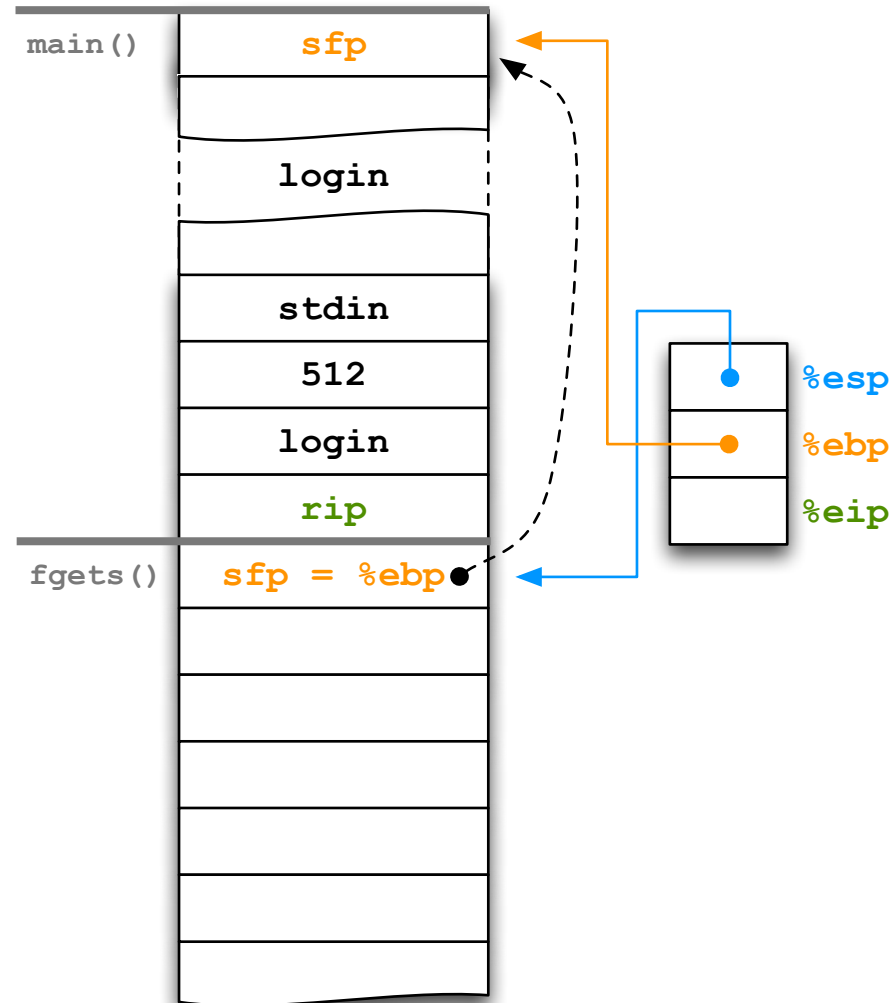
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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
stdin
512
login
rip

fgets()
sfp = %ebp

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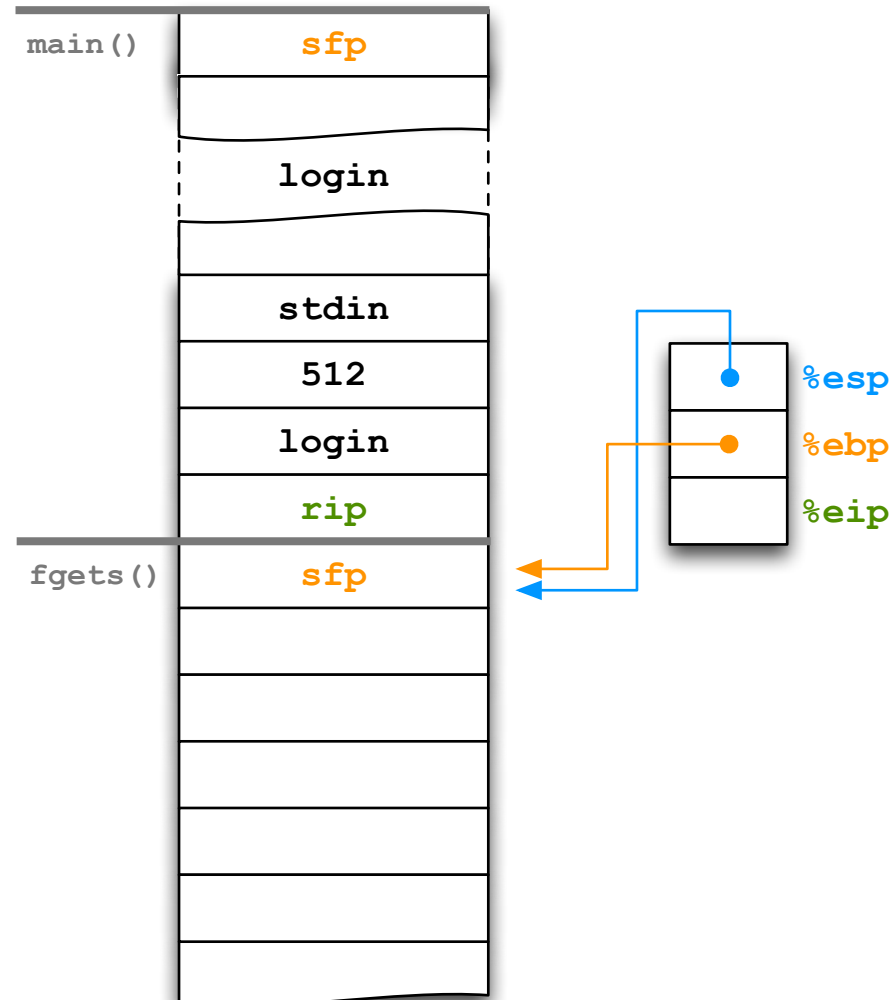
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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
stdin
512
login
rip

fgets()

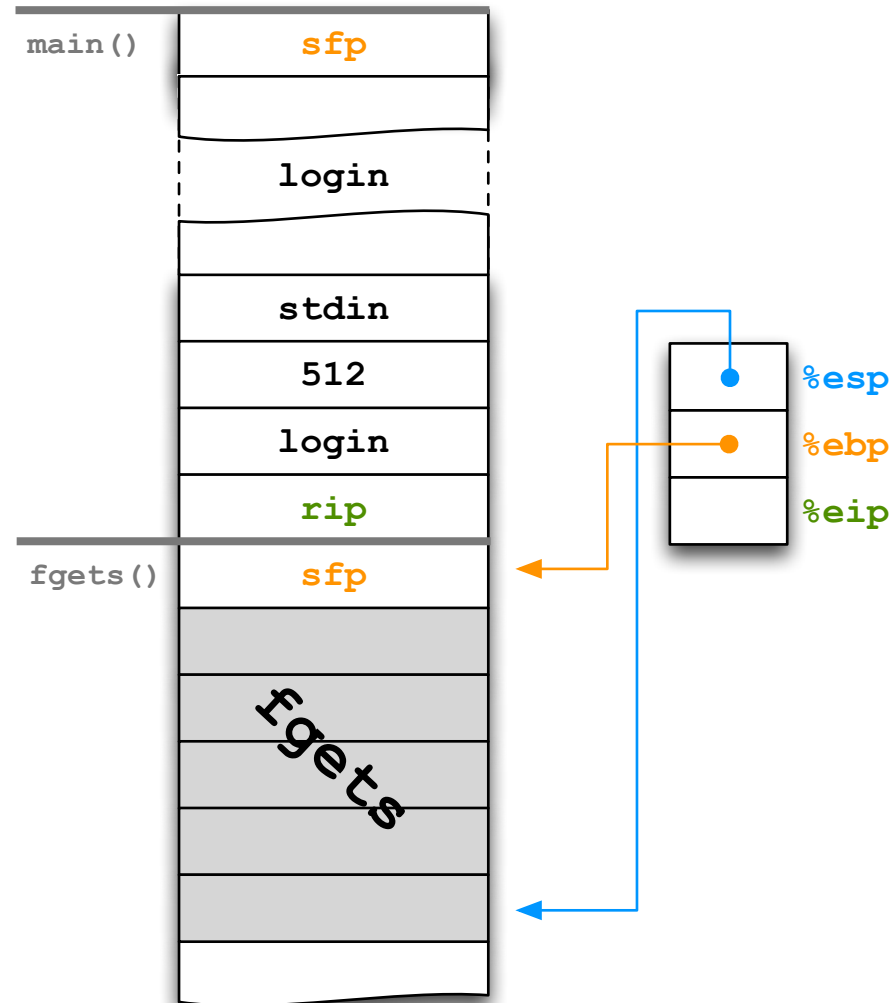| sfp |
| --- |

%esp
%ebp
%eip

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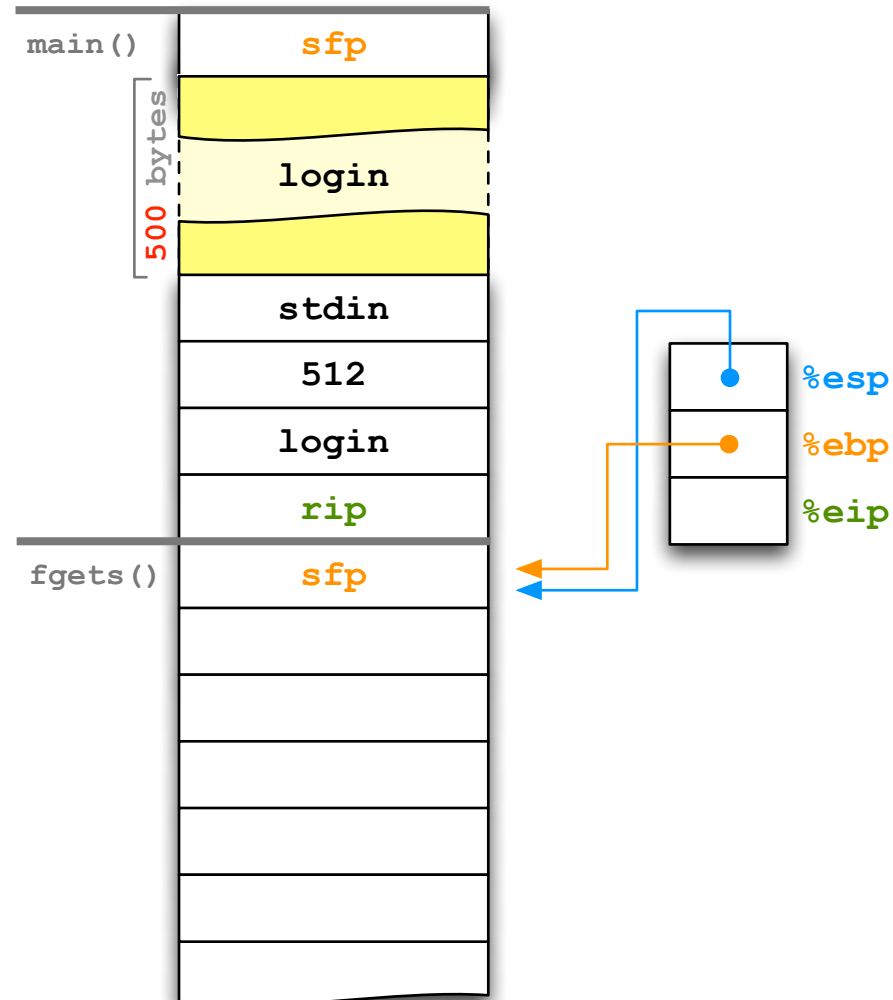
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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

500 bytes   login

stdin

512

login

rip

fgets()   sfp
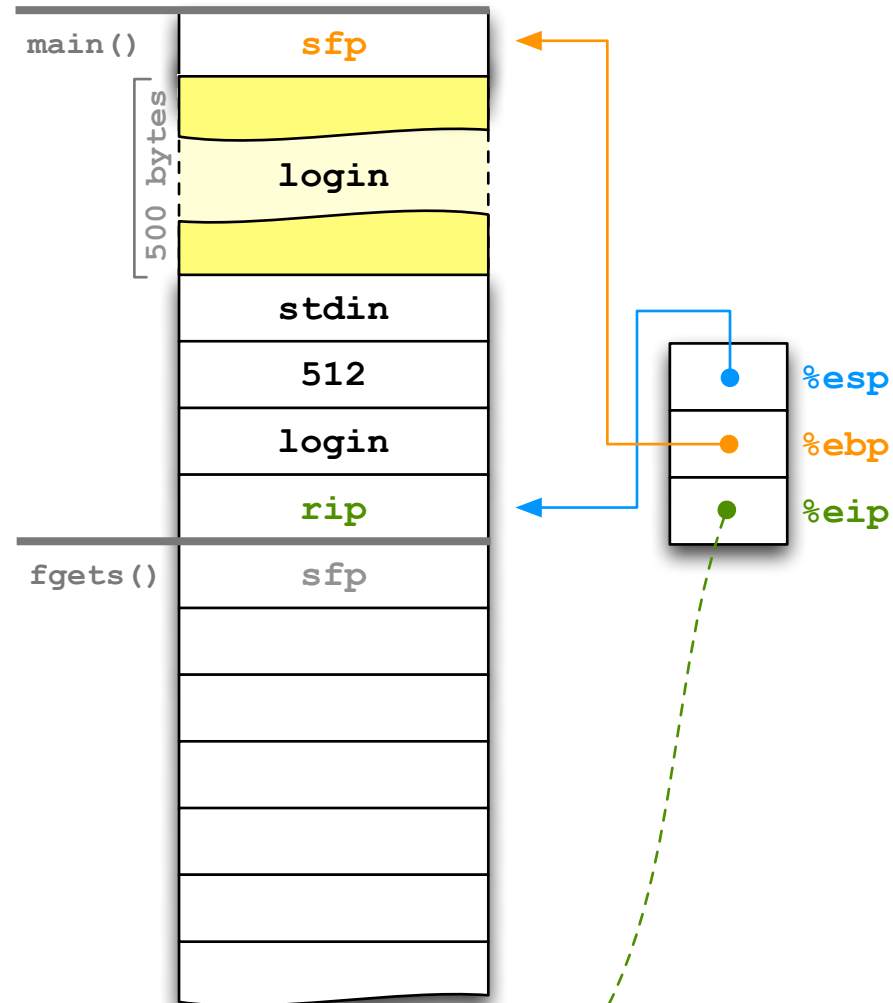
%esp
%ebp
%eip

```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

500 bytes   login

stdin

512

login

rip

fgets()   sfp
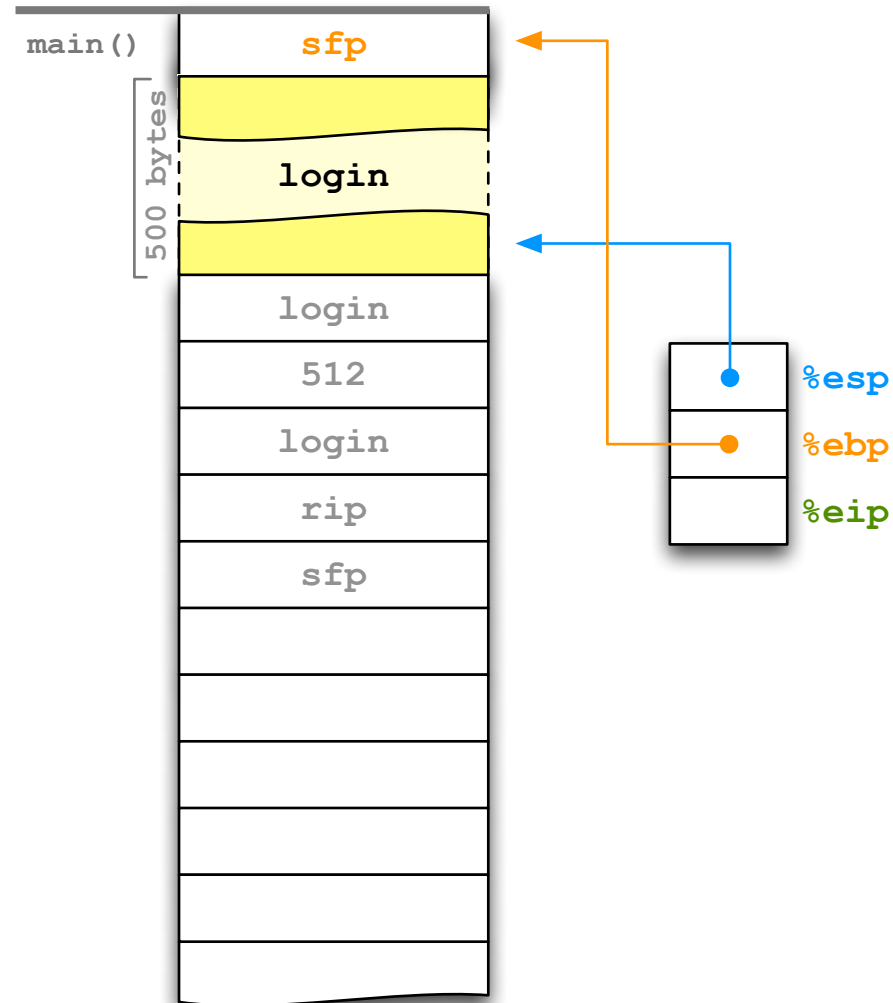
%esp
%ebp
%eip

```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
500 bytes	login
	login
	512
	login
	rip
	sfp

%esp
%ebp
%eip

```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;
}
```
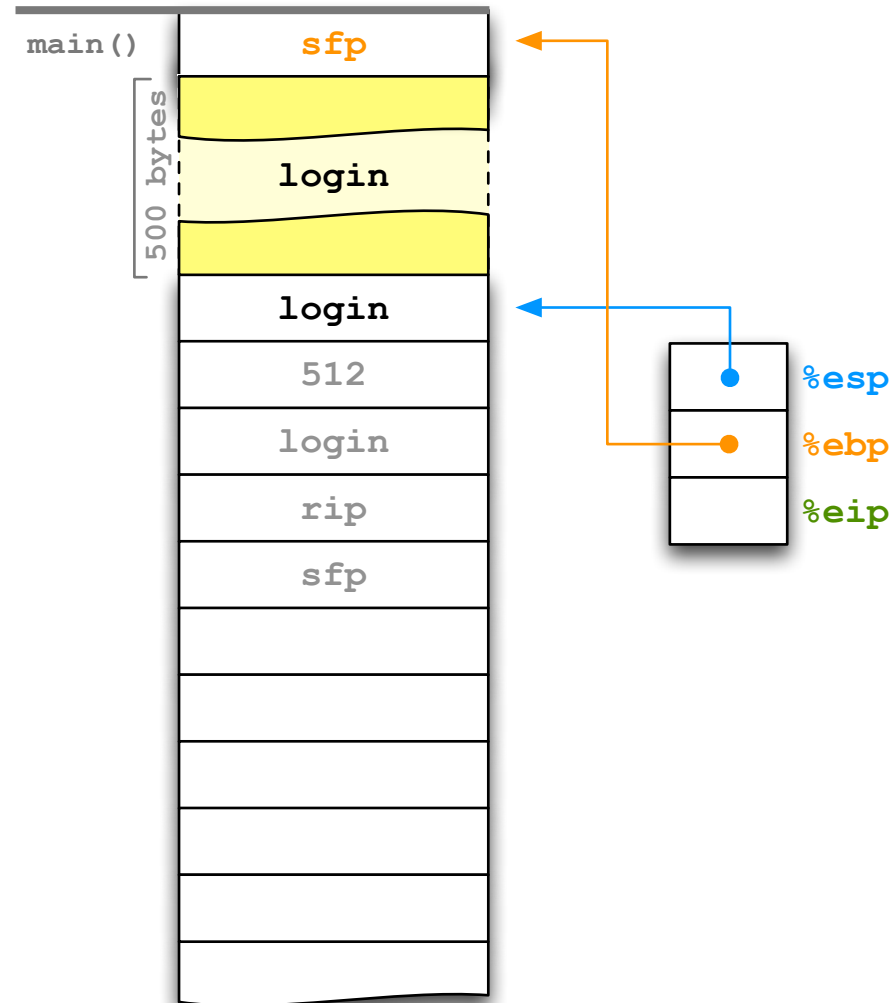
main()

sfp

500 bytes

login

login

512

login

rip

sfp

%esp

%ebp

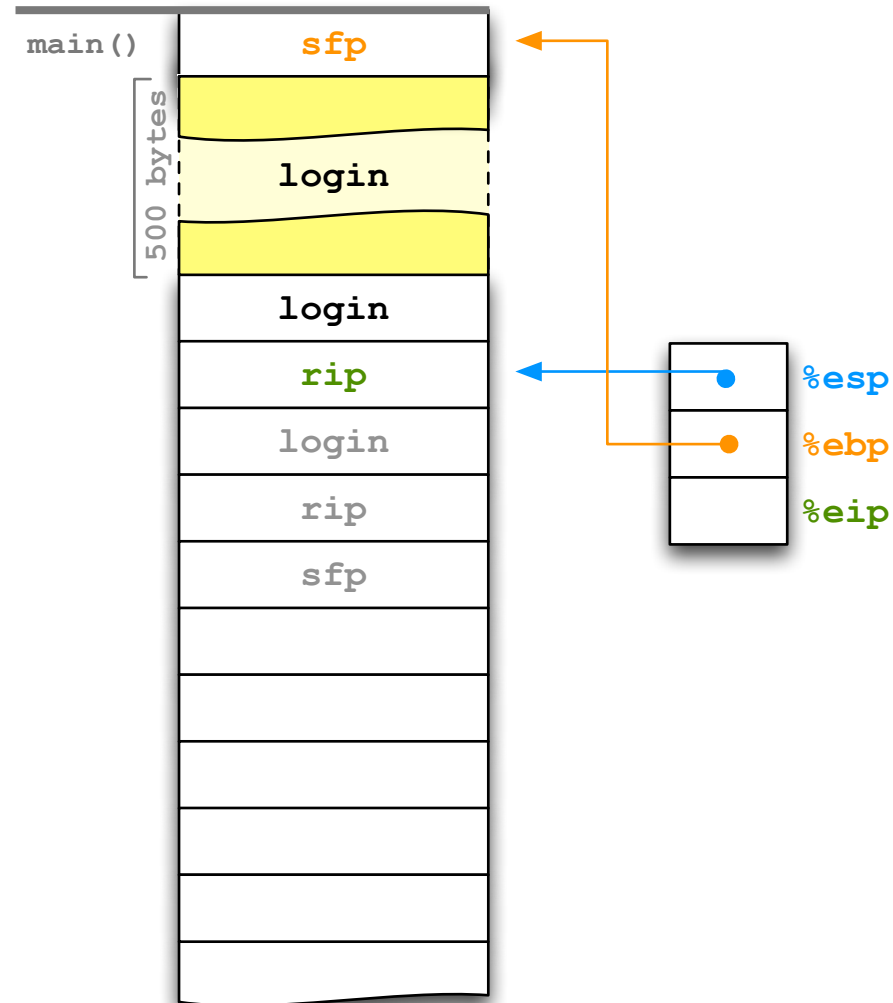%eip

```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

500 bytes

login

login

rip

login

rip

sfp

%esp

%ebp
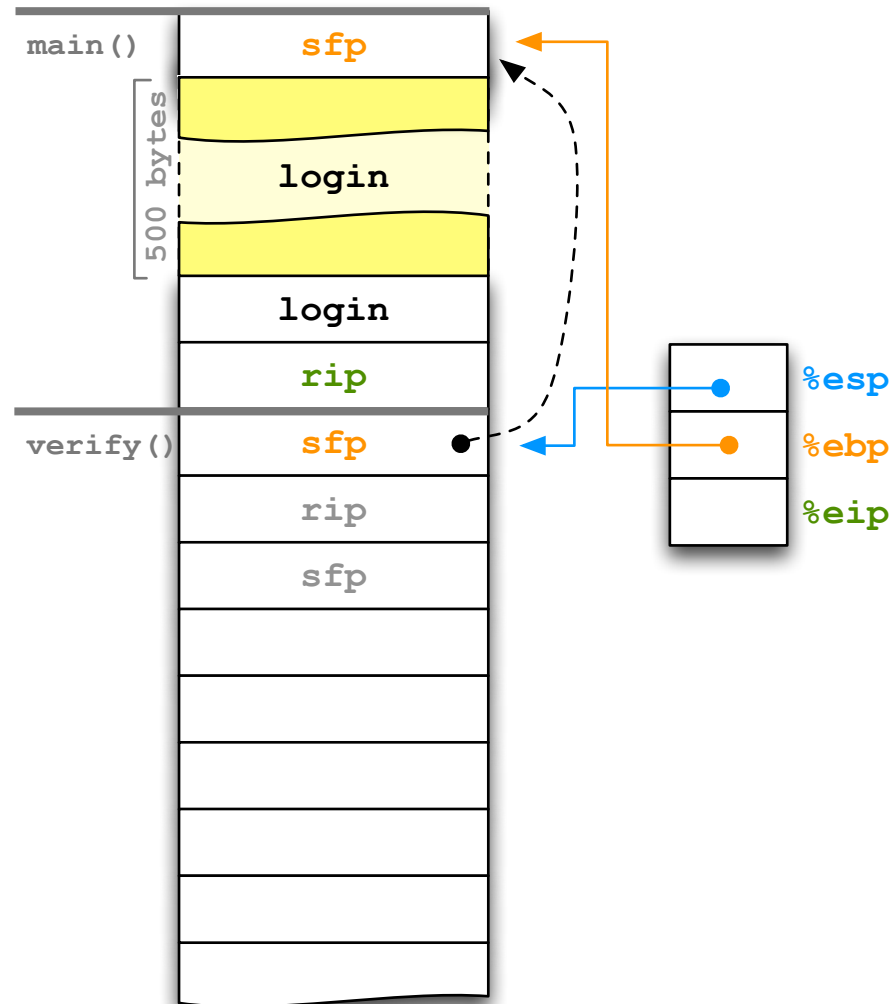
%eip

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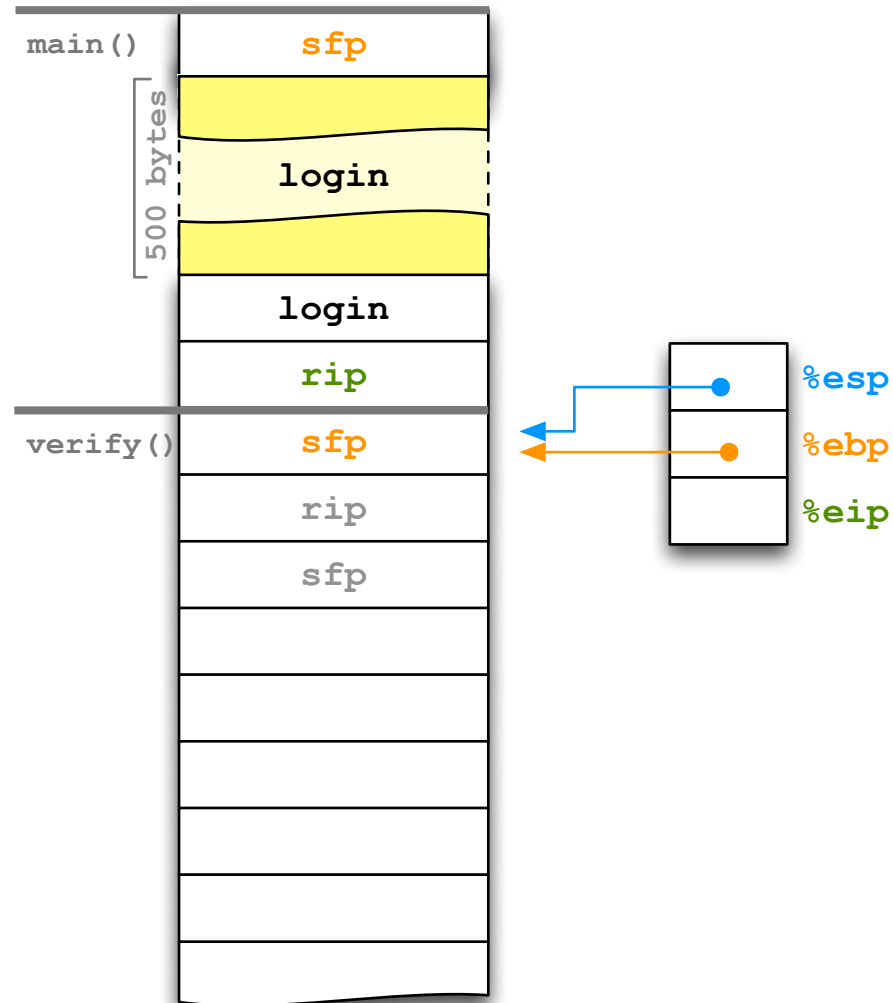
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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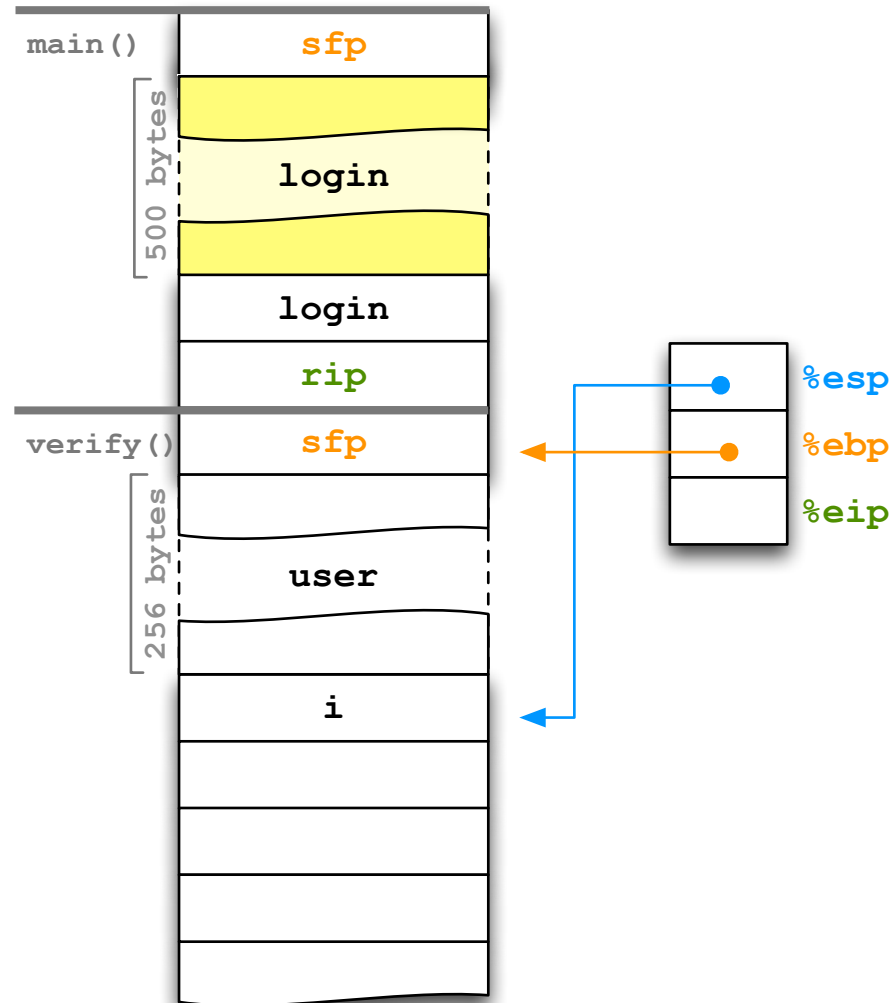
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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

500 bytes

login

login

rip

verify()

sfp

256 bytes

user

i

%esp

%ebp
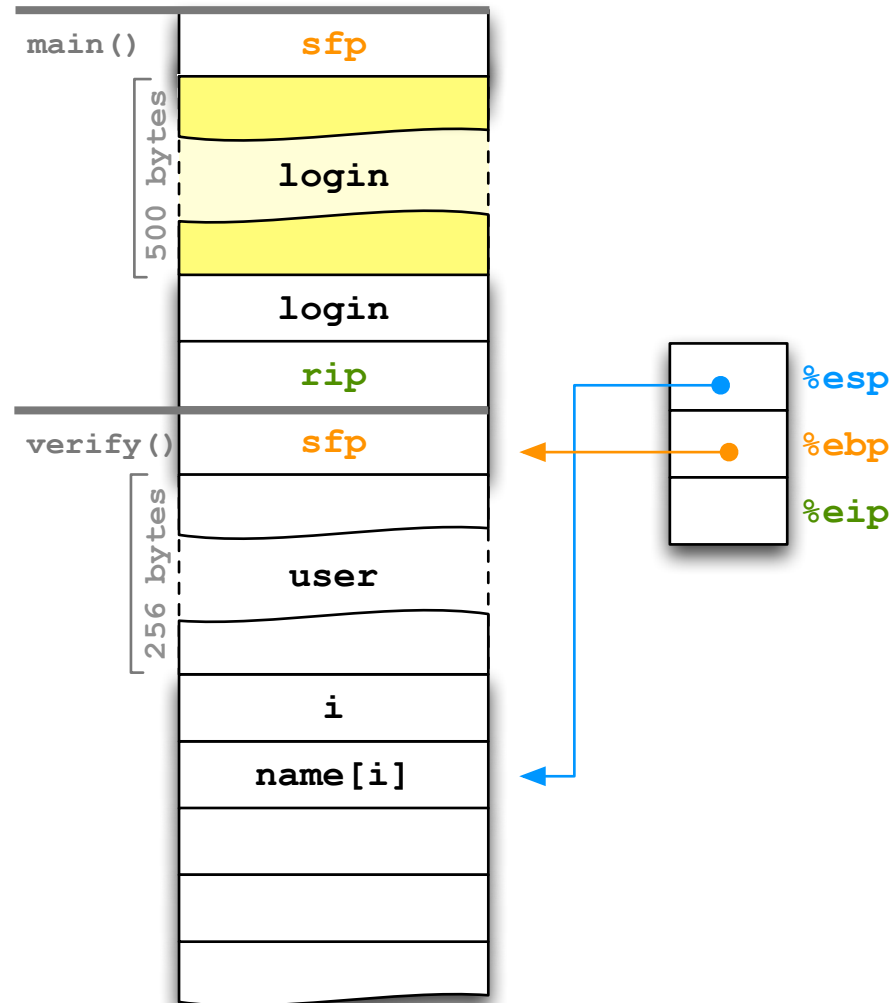
%eip

```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

500 bytes login

login

rip

verify() sfp

256 bytes user

i

name[i]

%esp

%ebp
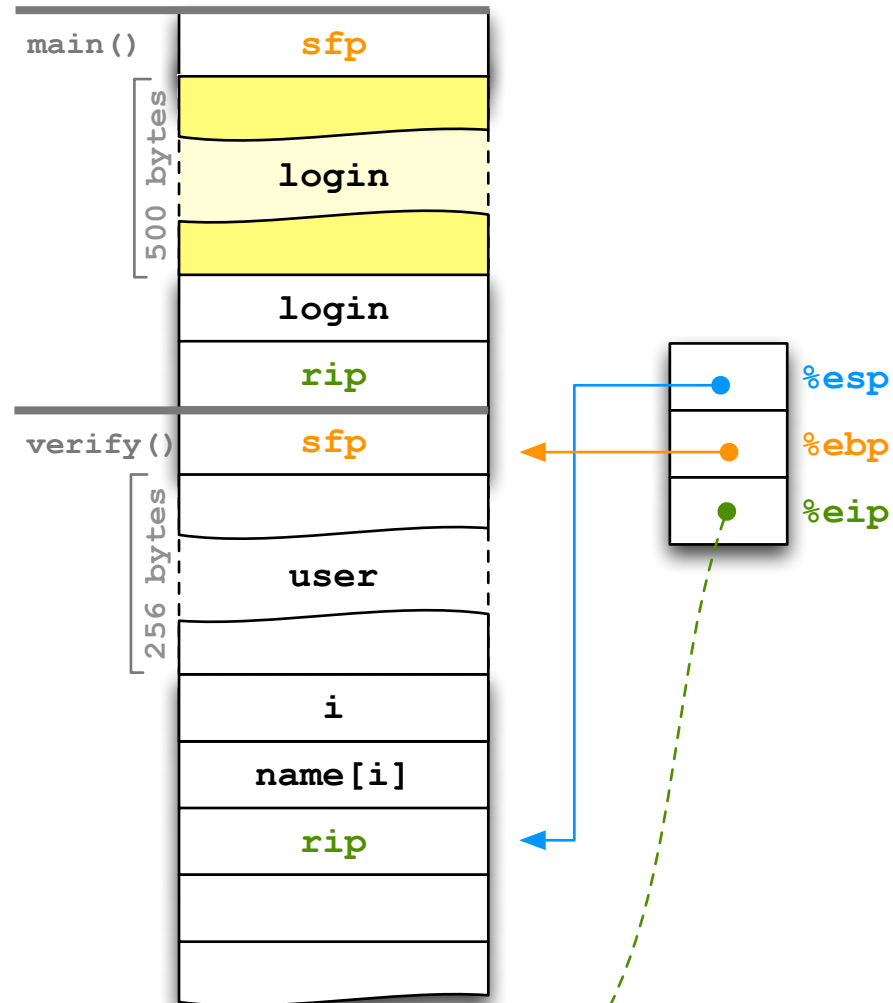
%eip

```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

500 bytes

login

login

rip

verify()

sfp

256 bytes

user

i

name[i]

rip

%esp

%ebp
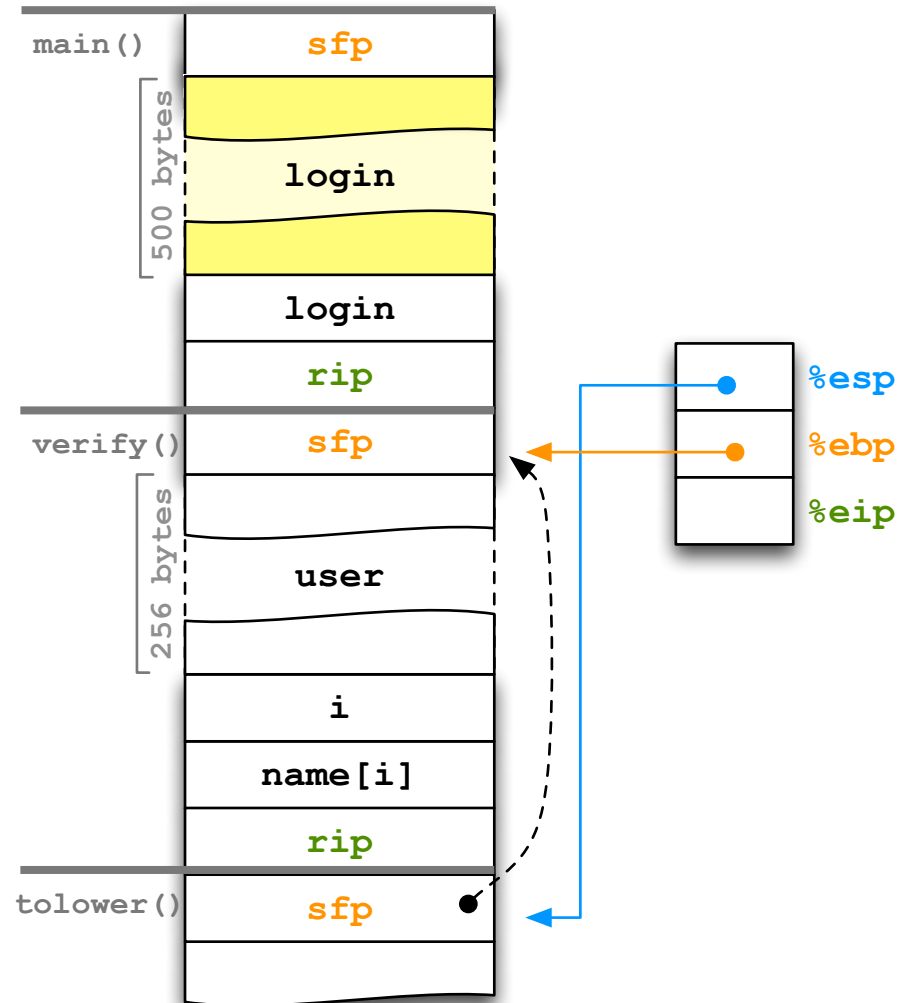
%eip

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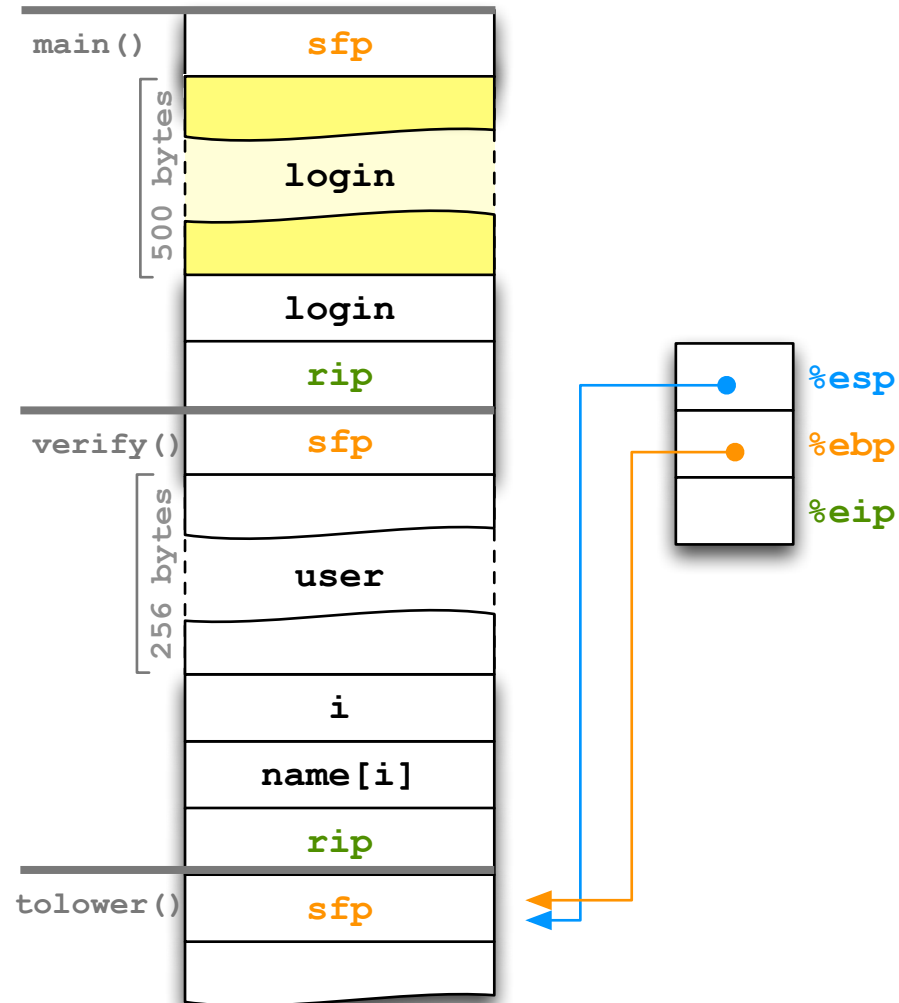
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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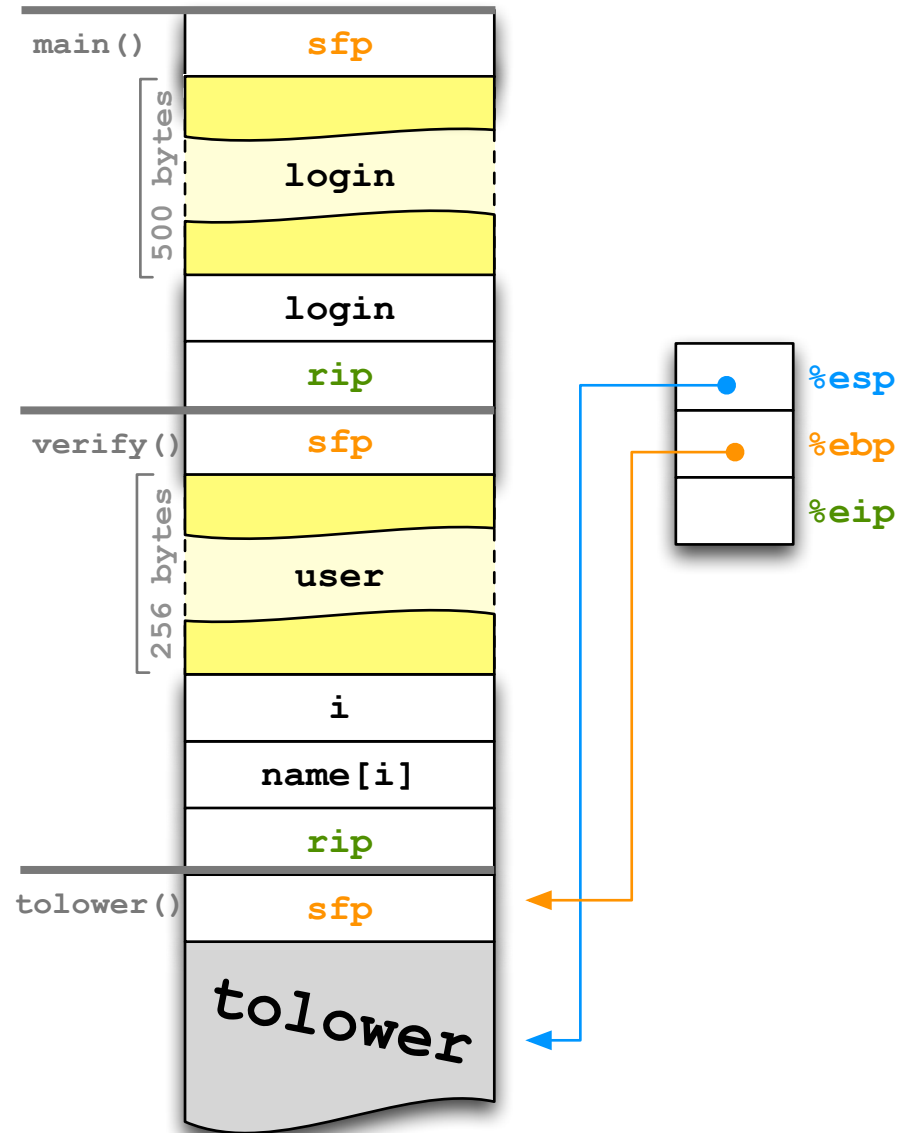
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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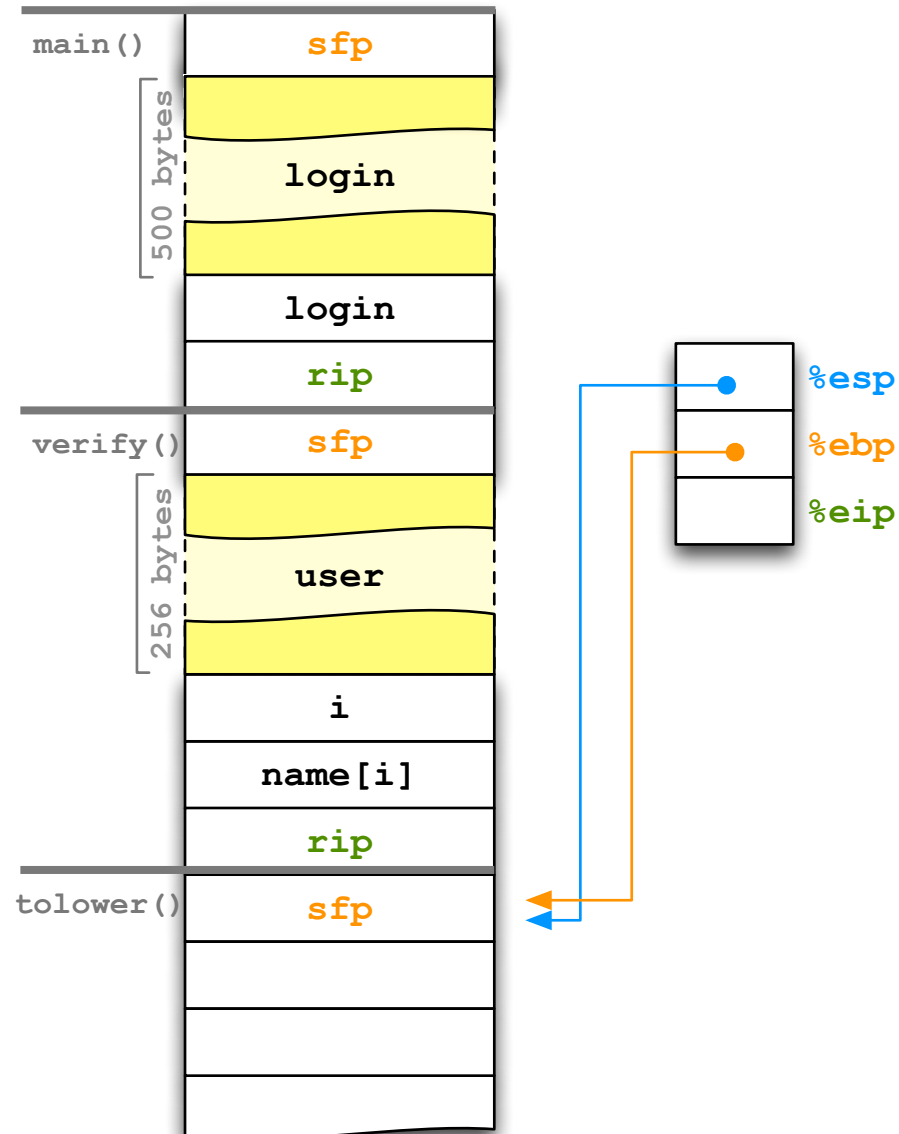
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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

500 bytes

login

login

rip

verify()

sfp

256 bytes

user

i

name[i]

rip

tolower()

sfp

%esp

%ebp
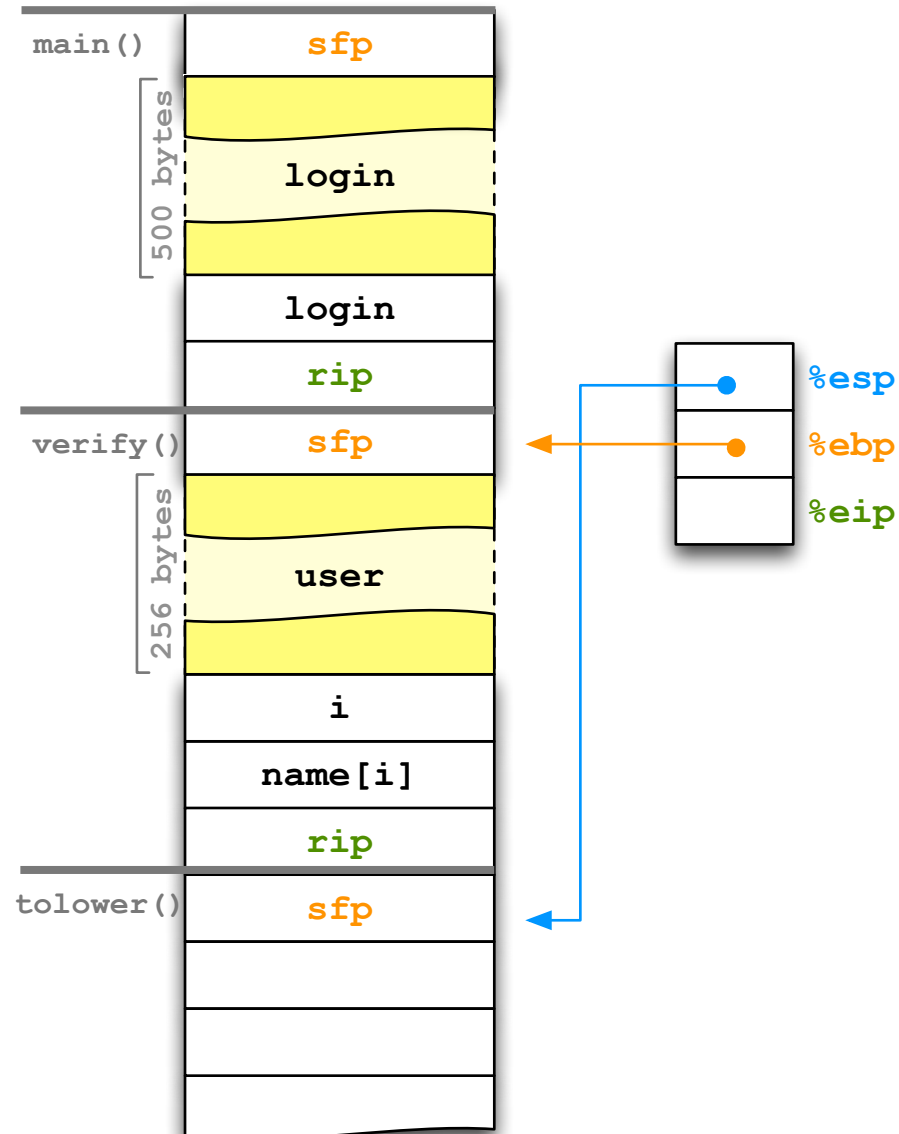
%eip

```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

500 bytes

login

login

rip

verify() sfp

256 bytes

user

i

name[i]

rip

tolower() sfp

%esp

%ebp
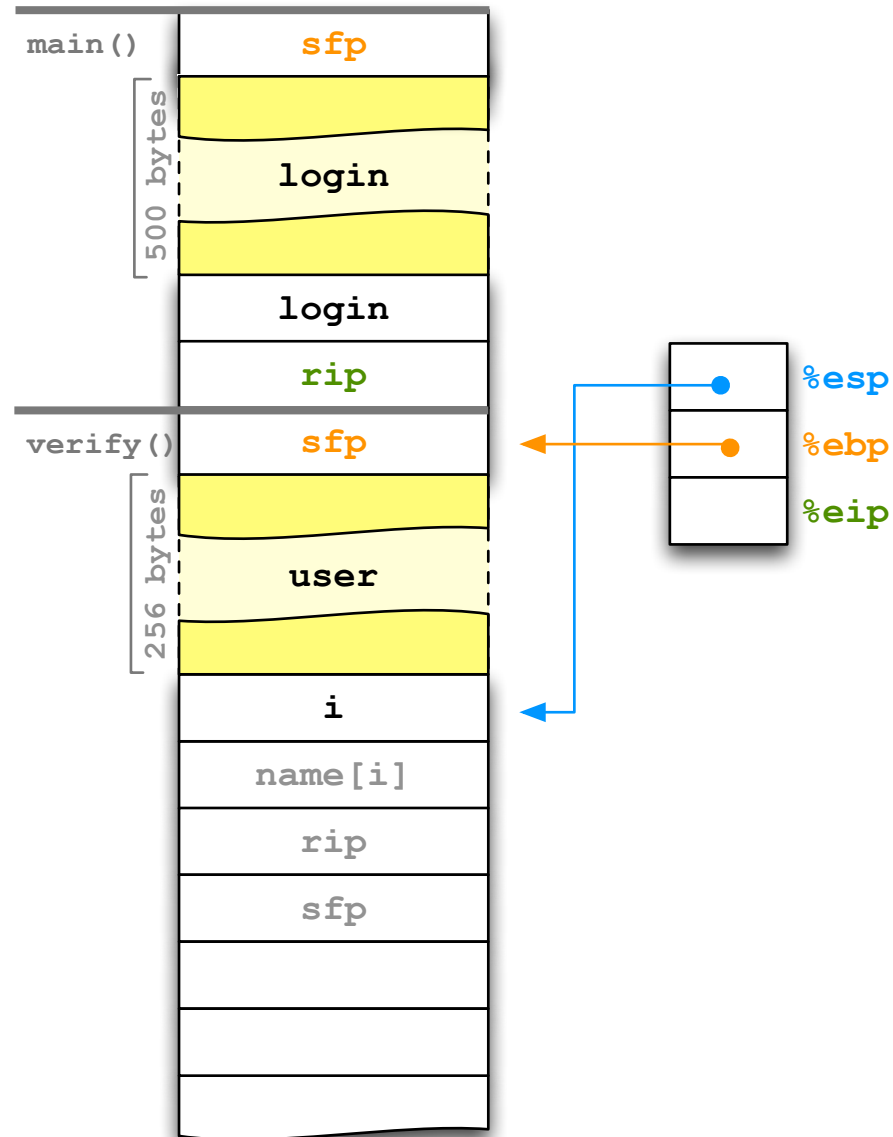
%eip

```
#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;
}
```

main()   sfp

500 bytes
login

login

rip

verify()   sfp

256 bytes
user

i

name[i]

rip

sfp

%esp

%ebp
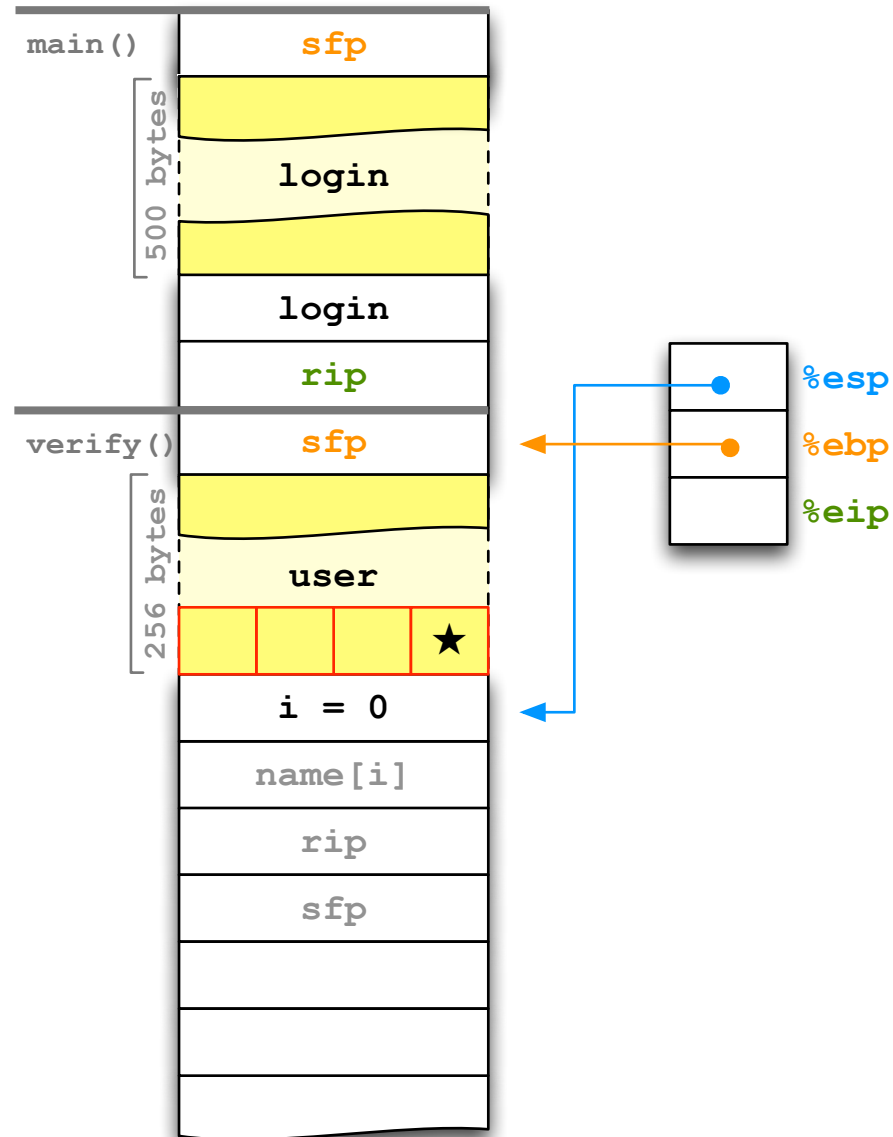
%eip

```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

500 bytes

login

login

rip

verify() sfp

256 bytes

user

★

i = 0

name[i]

rip

sfp

%esp

%ebp
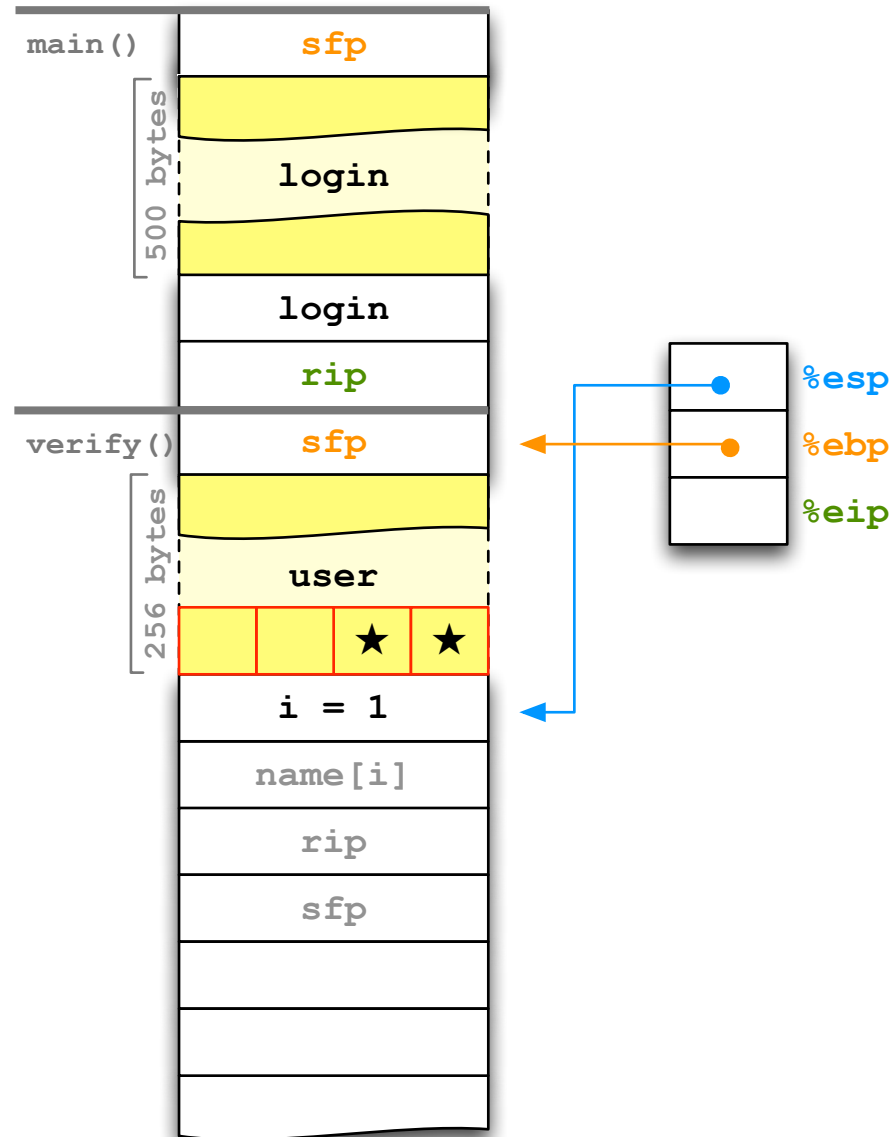
%eip

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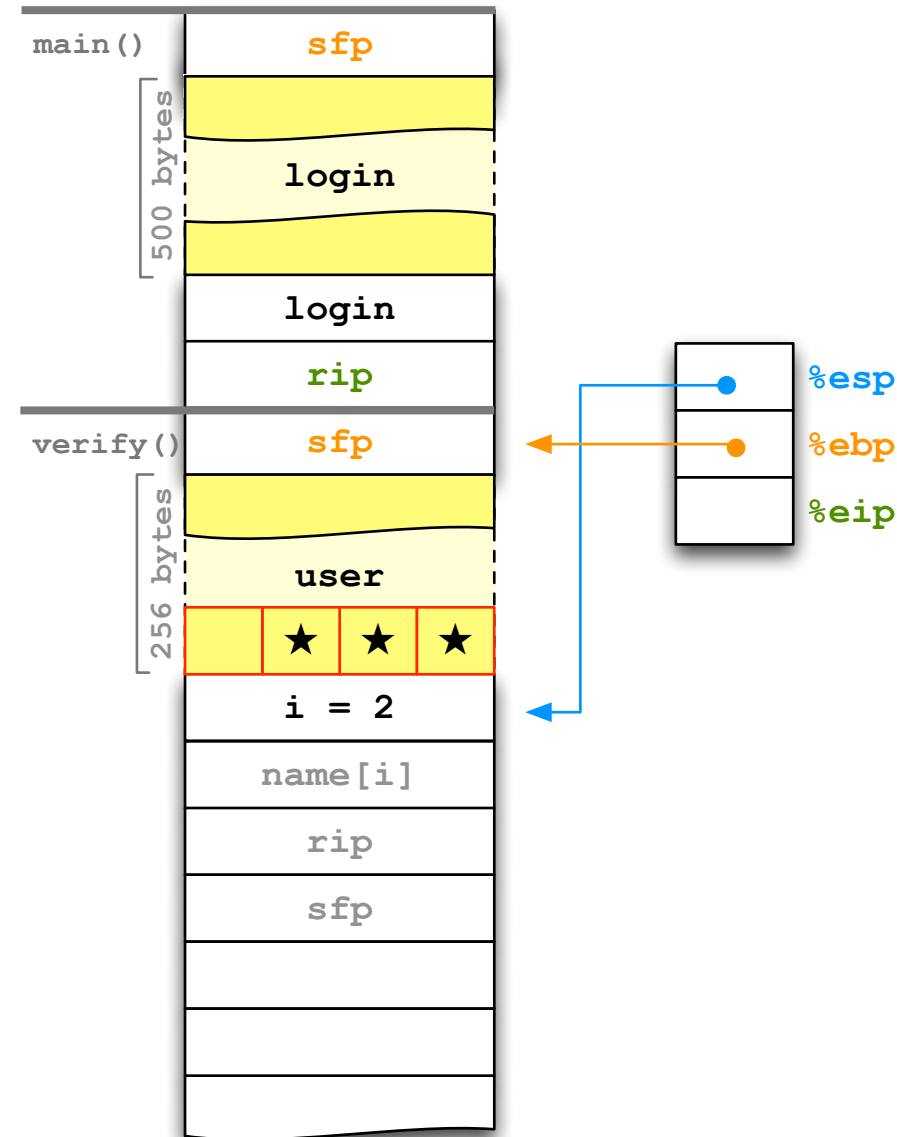
```c
#include <ctype.h>   // tolower
#include <string.h>  // strcmp
#include <stdio.h>   // fgets, fputs

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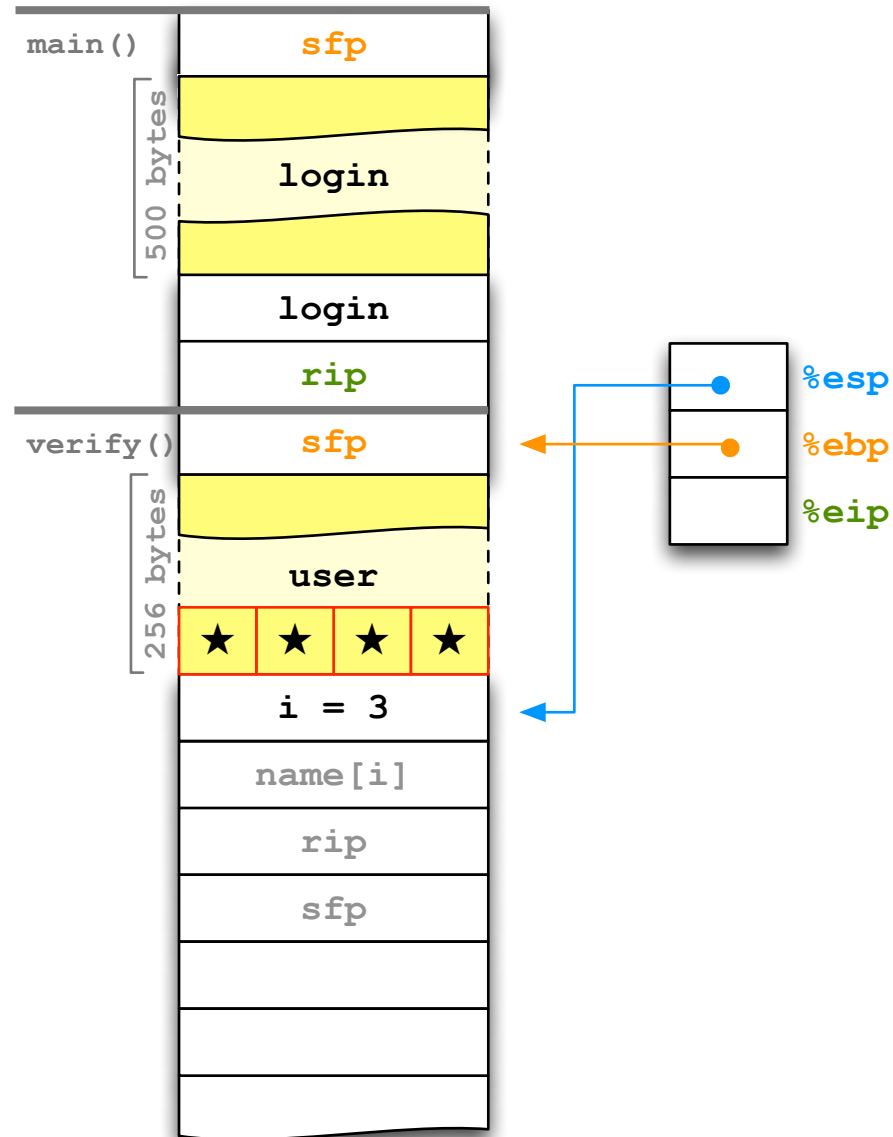
```c
#include <ctype.h>   // tolower
#include <string.h>  // strcmp
#include <stdio.h>   // fgets, fputs

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

500 bytes

login

login

rip

verify()

sfp

256 bytes

user

★ ★ ★ ★

i = 3

name[i]

rip

sfp

%esp
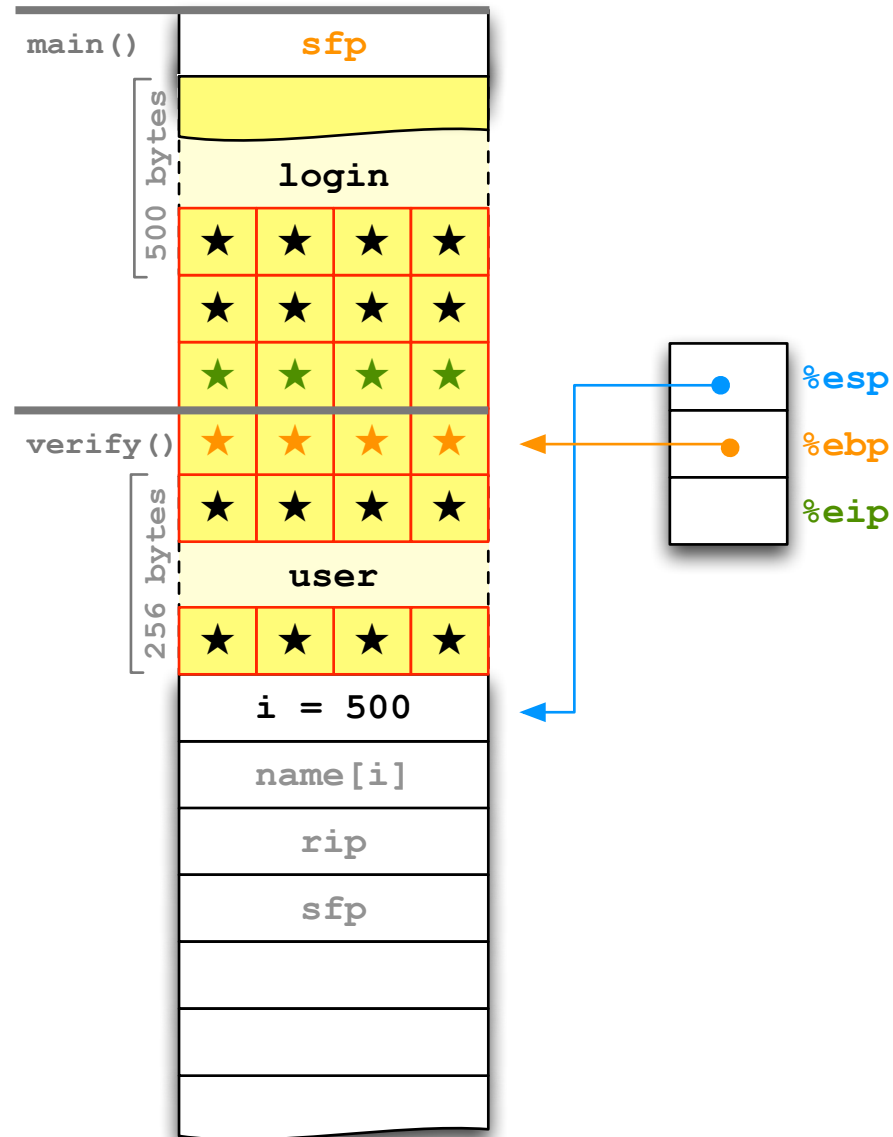%ebp
%eip

```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

500 bytes

login

★ ★ ★ ★
★ ★ ★ ★
★ ★ ★ ★

verify() ★ ★ ★ ★   %ebp

%esp

256 bytes
★ ★ ★ ★

user

★ ★ ★ ★

%eip

i = 500

name[i]

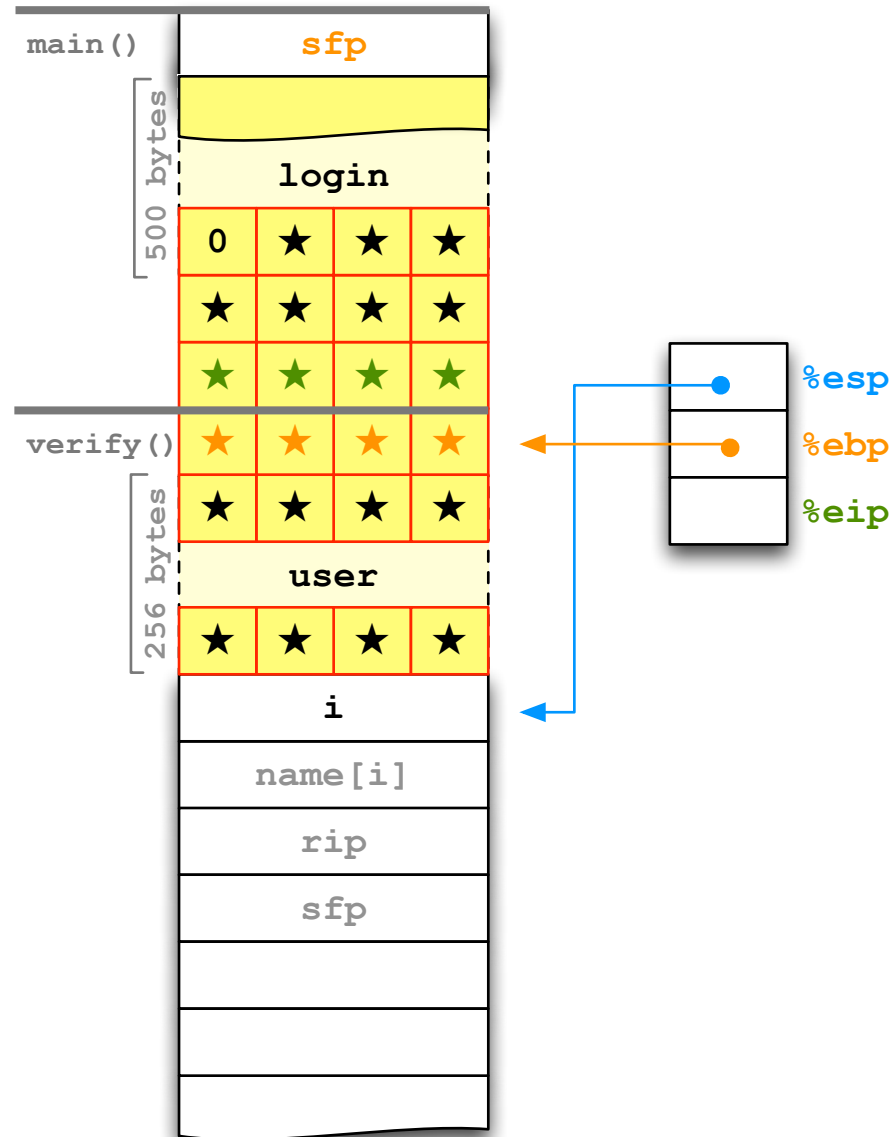rip

sfp

```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

500 bytes

login

0	★	★	★
★	★	★	★
★	★	★	★

%esp

verify()

| ★ | ★ | ★ | ★ |
| ★ | ★ | ★ | ★ |

%ebp

256 bytes

user

| ★ | ★ | ★ | ★ |

%eip

i

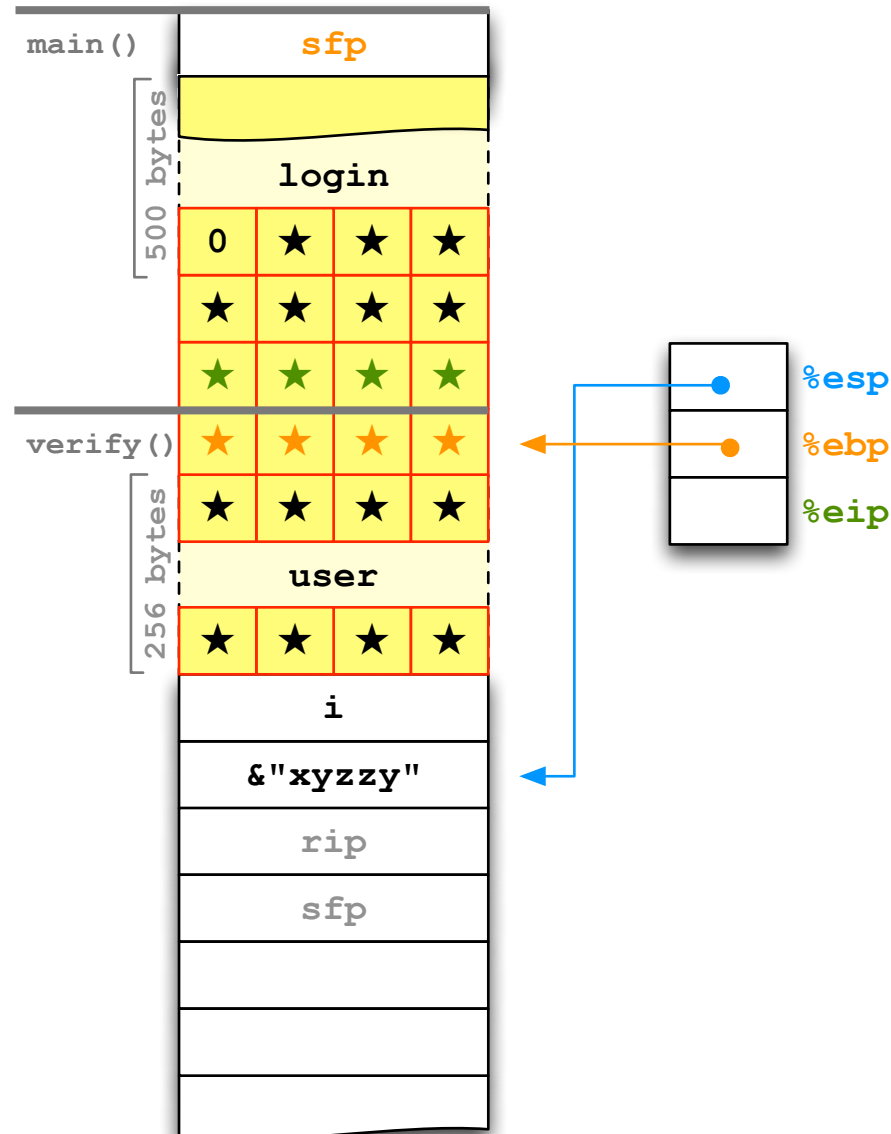name[i]

rip

sfp

```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

500 bytes

login

0 ★ ★ ★
★ ★ ★ ★
★ ★ ★ ★

verify()
★ ★ ★ ★

256 bytes

★ ★ ★ ★

user

★ ★ ★ ★

i

&"xyzzy"

rip

sfp

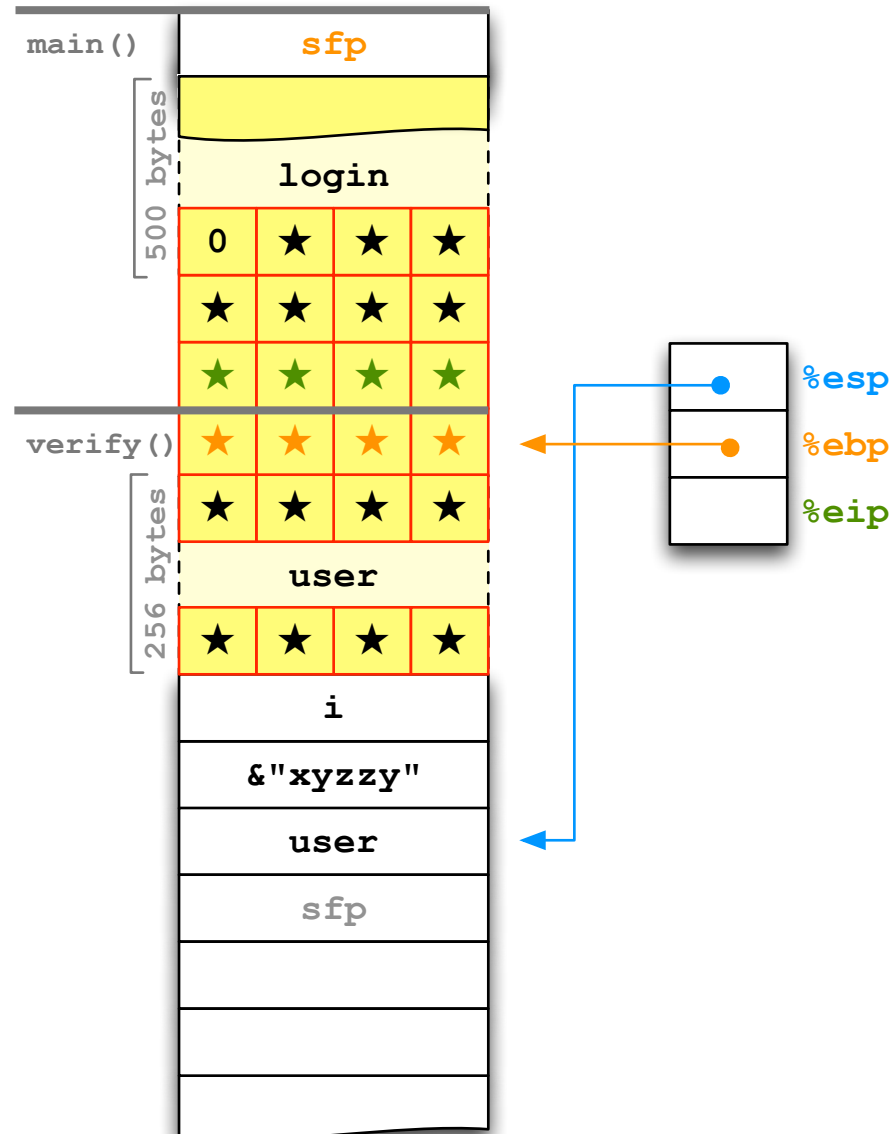%esp
%ebp
%eip

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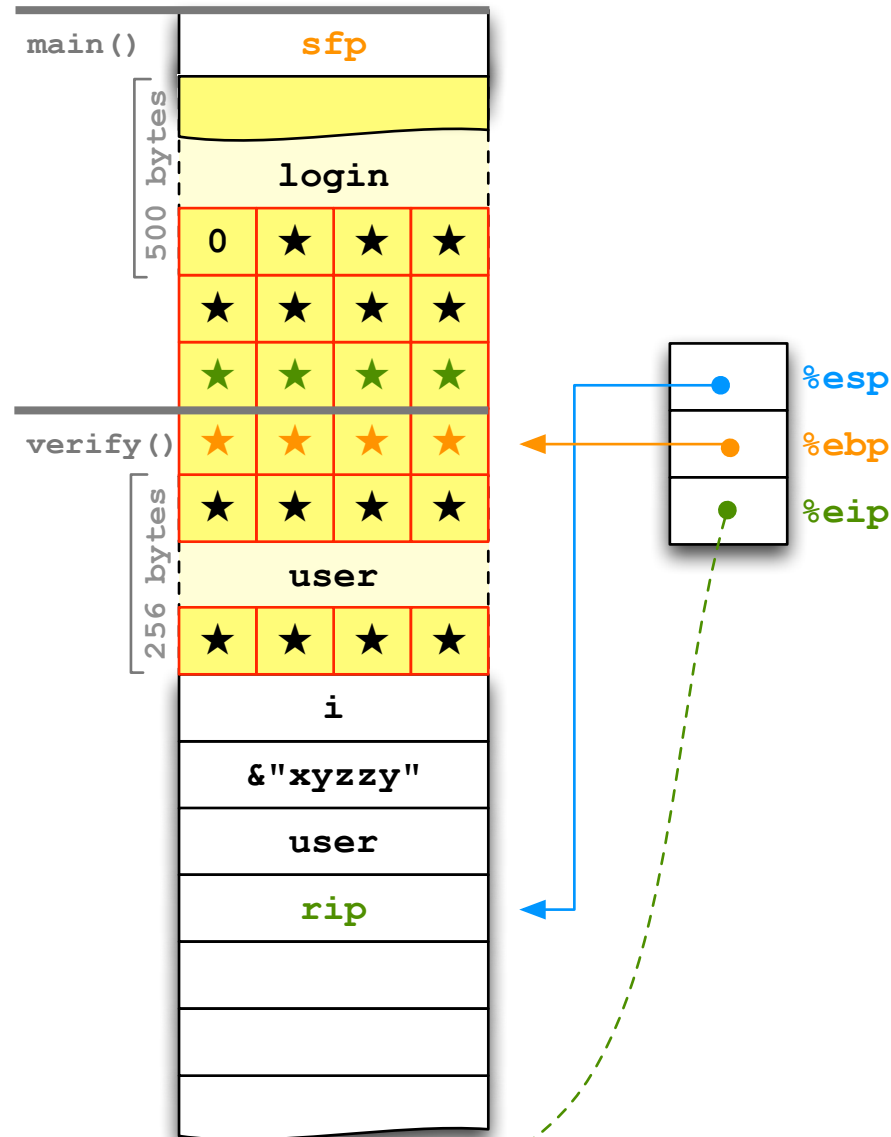
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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

500 bytes

login

0	★	★	★
★	★	★	★
★	★	★	★

verify()

| ★ | ★ | ★ | ★ |
| ★ | ★ | ★ | ★ |

256 bytes

user

| ★ | ★ | ★ | ★ |

| i |
| &"xyzzy" |
| user |
| rip |

%esp
%ebp
%eip

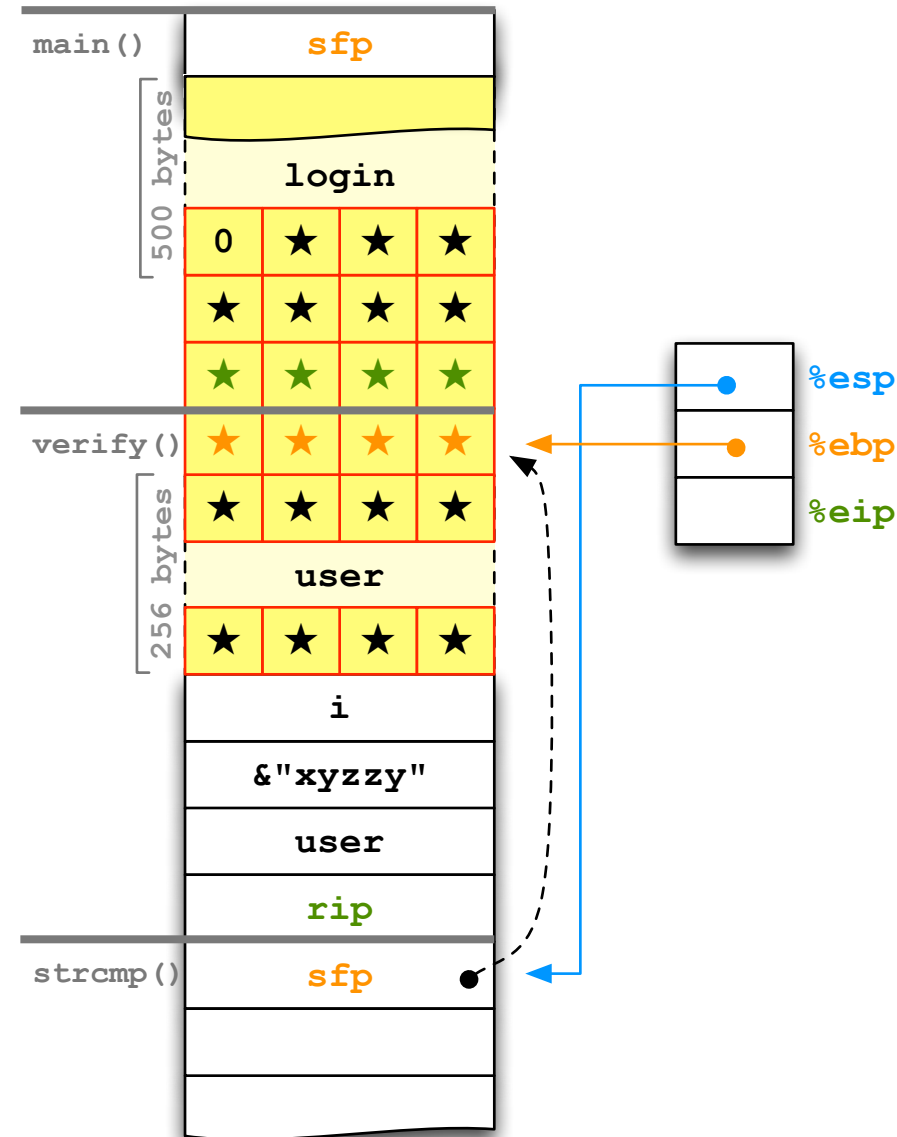```c
#include <ctype.h> // tolower
#include <string.h> // strcmp
#include <stdio.h> // fgets, fputs

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**

500 bytes — **login**

0	★	★	★
★	★	★	★
★	★	★	★

verify()

| ★ | ★ | ★ | ★ |
| ★ | ★ | ★ | ★ |

256 bytes — **user**

| ★ | ★ | ★ | ★ |

i

&"xyzzy"

user

rip

strcmp()   **sfp**

%esp

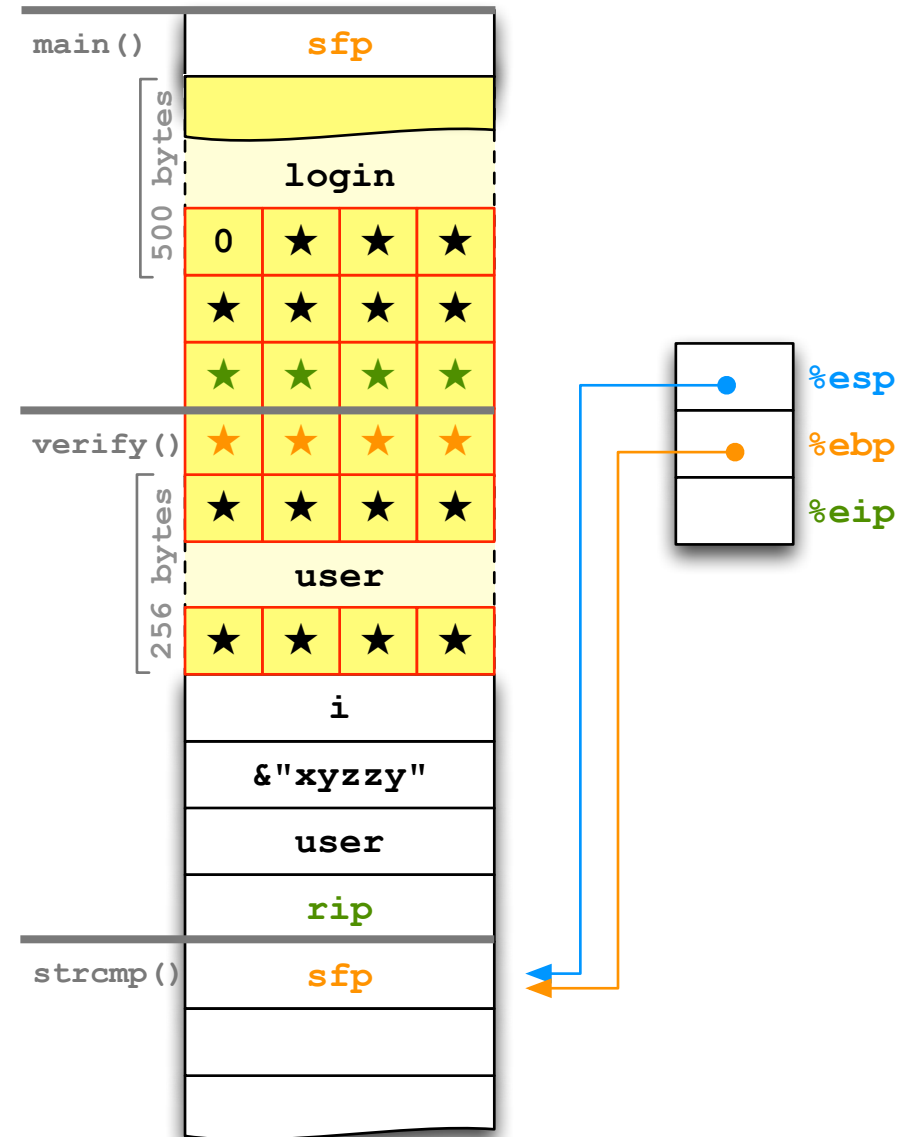%ebp
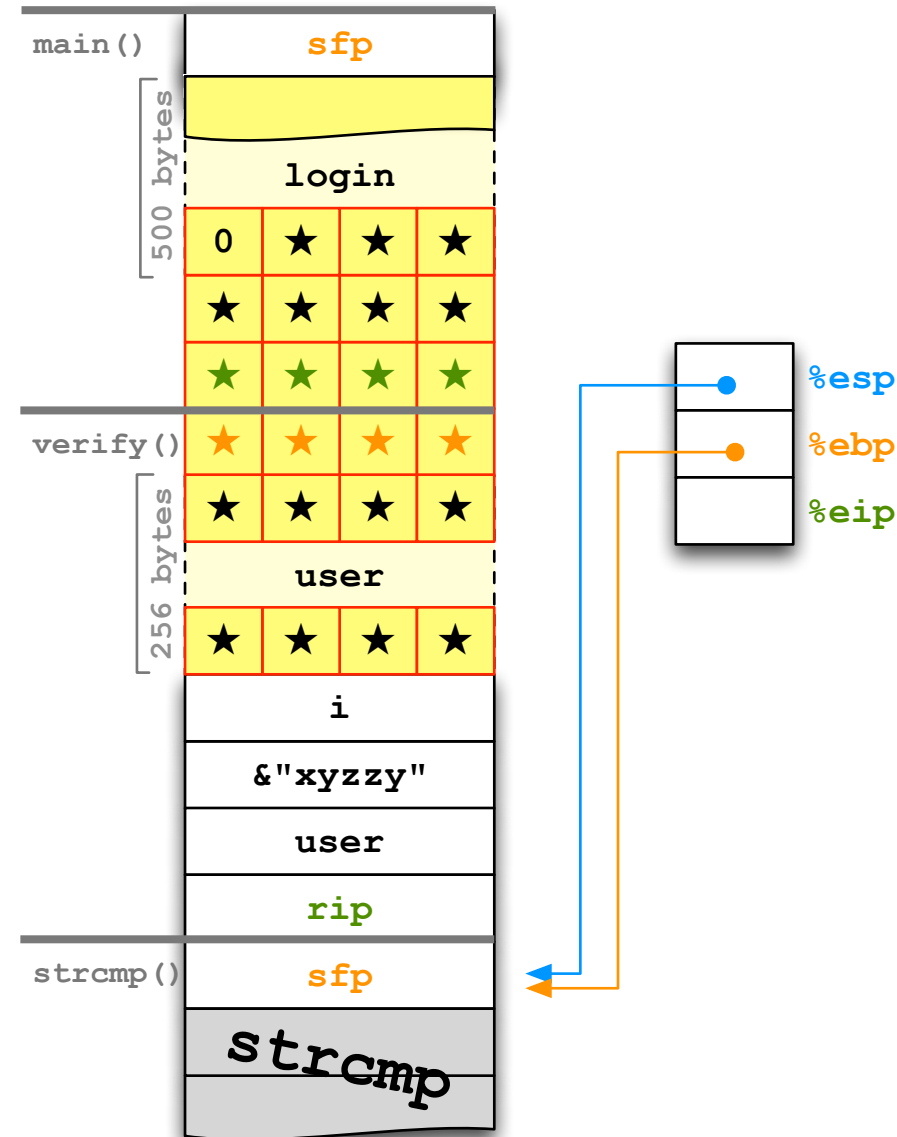
%eip

```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

500 bytes login

0	★	★	★
★	★	★	★
★	★	★	★

verify()

| ★ | ★ | ★ | ★ |
| ★ | ★ | ★ | ★ |

256 bytes user

| ★ | ★ | ★ | ★ |

i

&"xyzzy"

user

rip

strcmp() sfp

%esp

%ebp
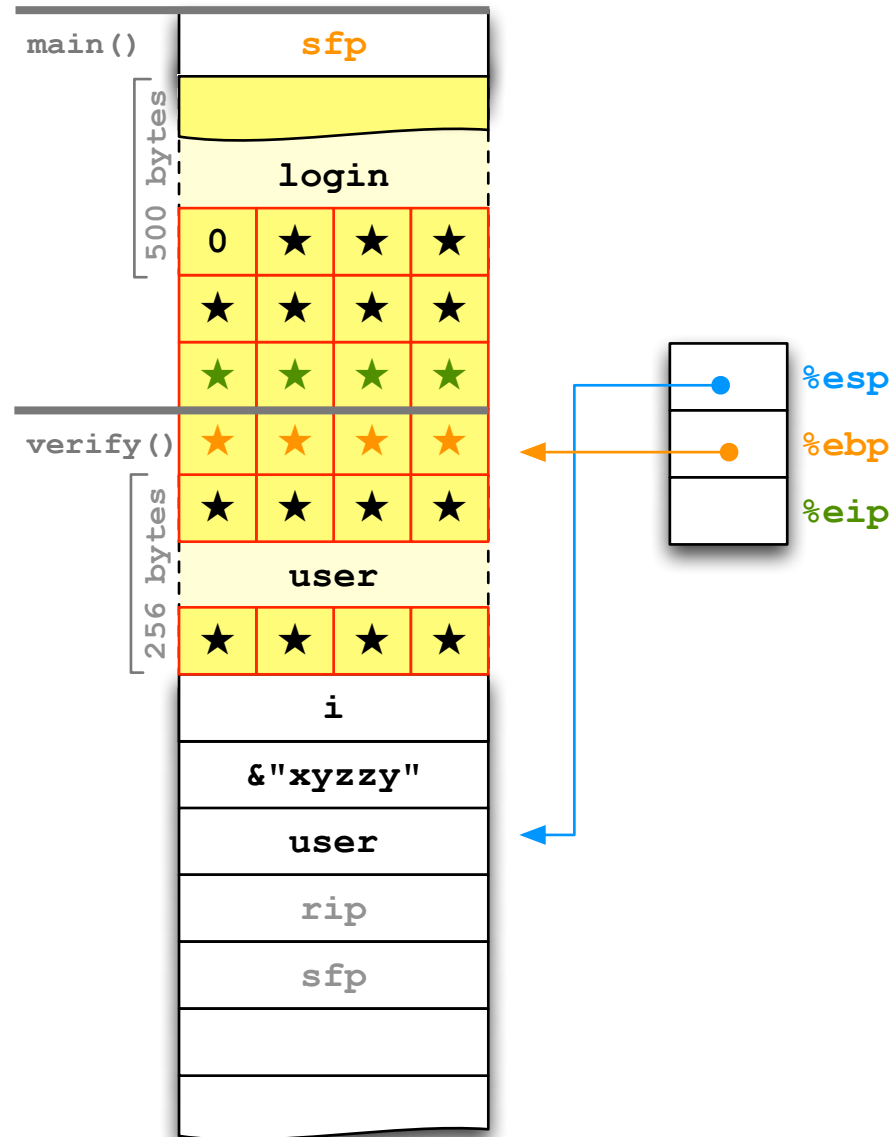
%eip

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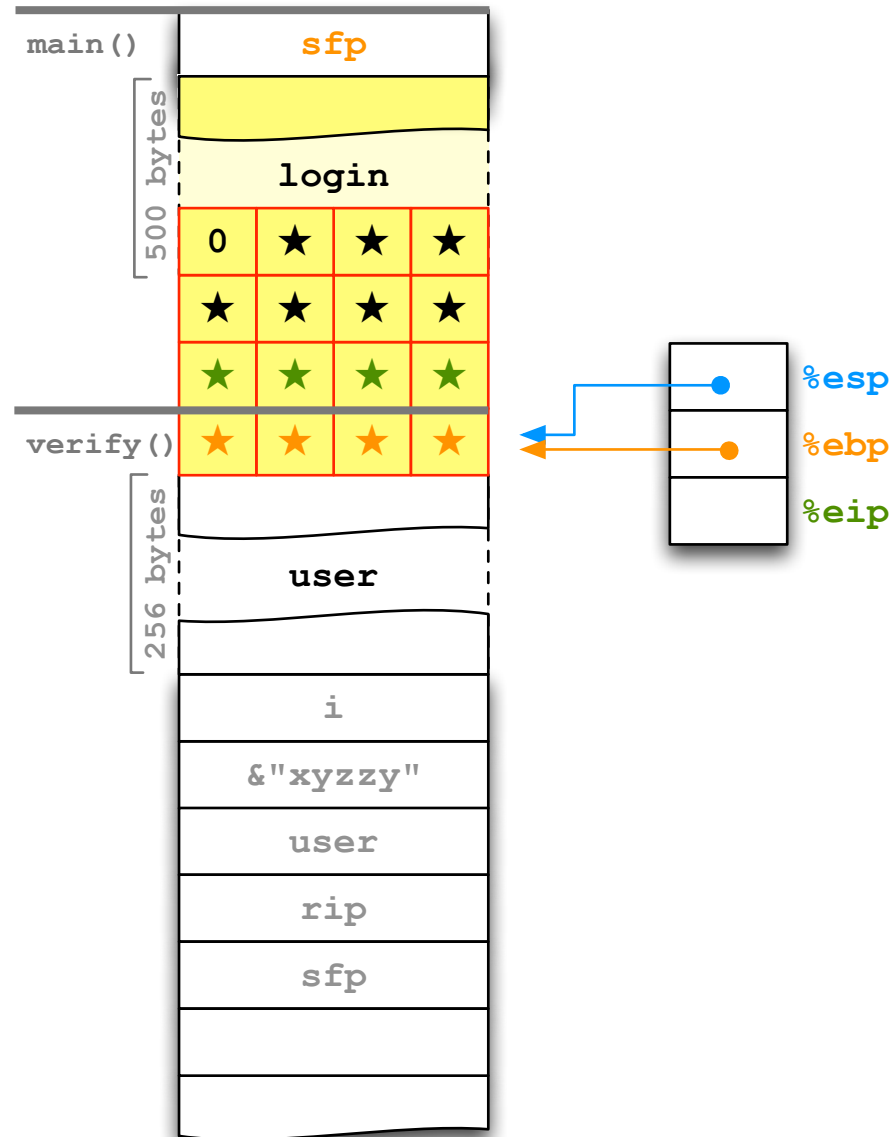
```c
#include <ctype.h>   // tolower
#include <string.h> // strcmp
#include <stdio.h>   // fgets, fputs

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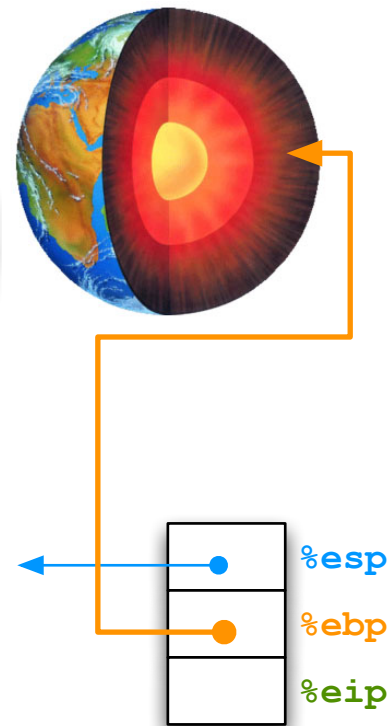
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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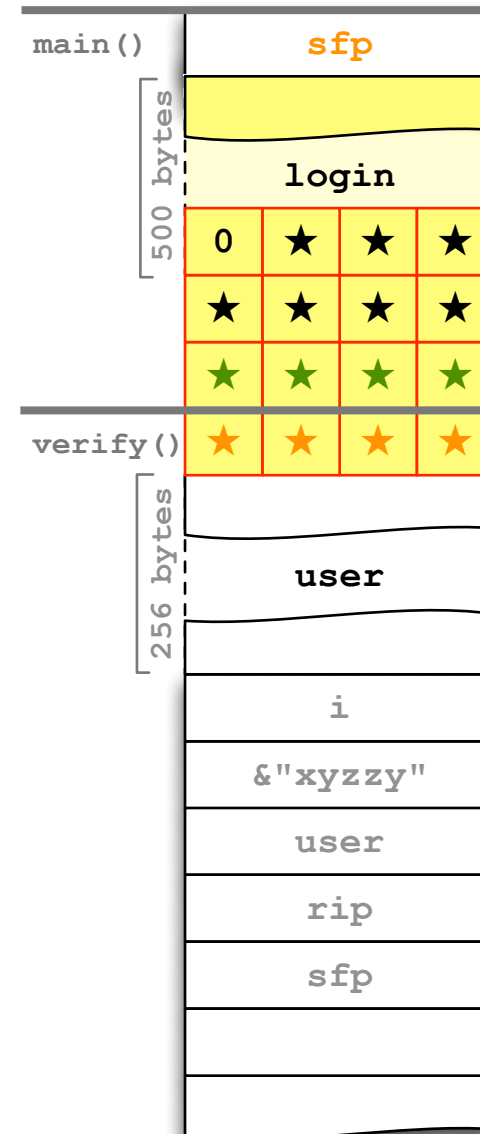
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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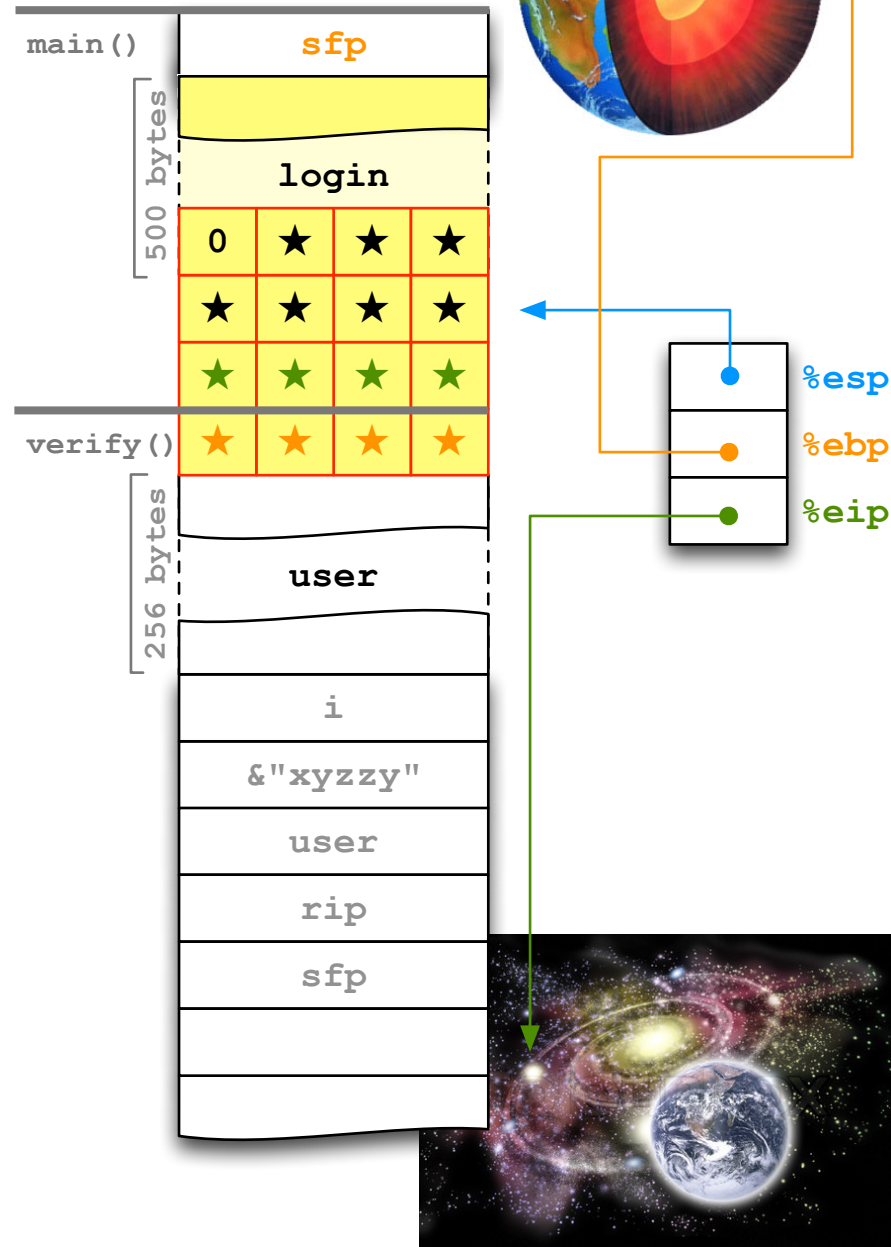
```c
#include <ctype.h>  // tolower
#include <string.h> // strcmp
#include <stdio.h>  // fgets, fputs

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 SECRE

}


int verify(
{

  char u
  int i;
  for
    user
  user
  retu

}


int main()
{
  char logi
  fgets(log
  if (! ve
    return 1;
  reveal_secre
  return 0;
}
```

main()

sfp

login

★

%esp
%ebp
%eip