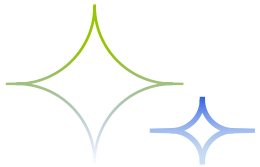


MONTANA
STATE UNIVERSITY

Programming with C I

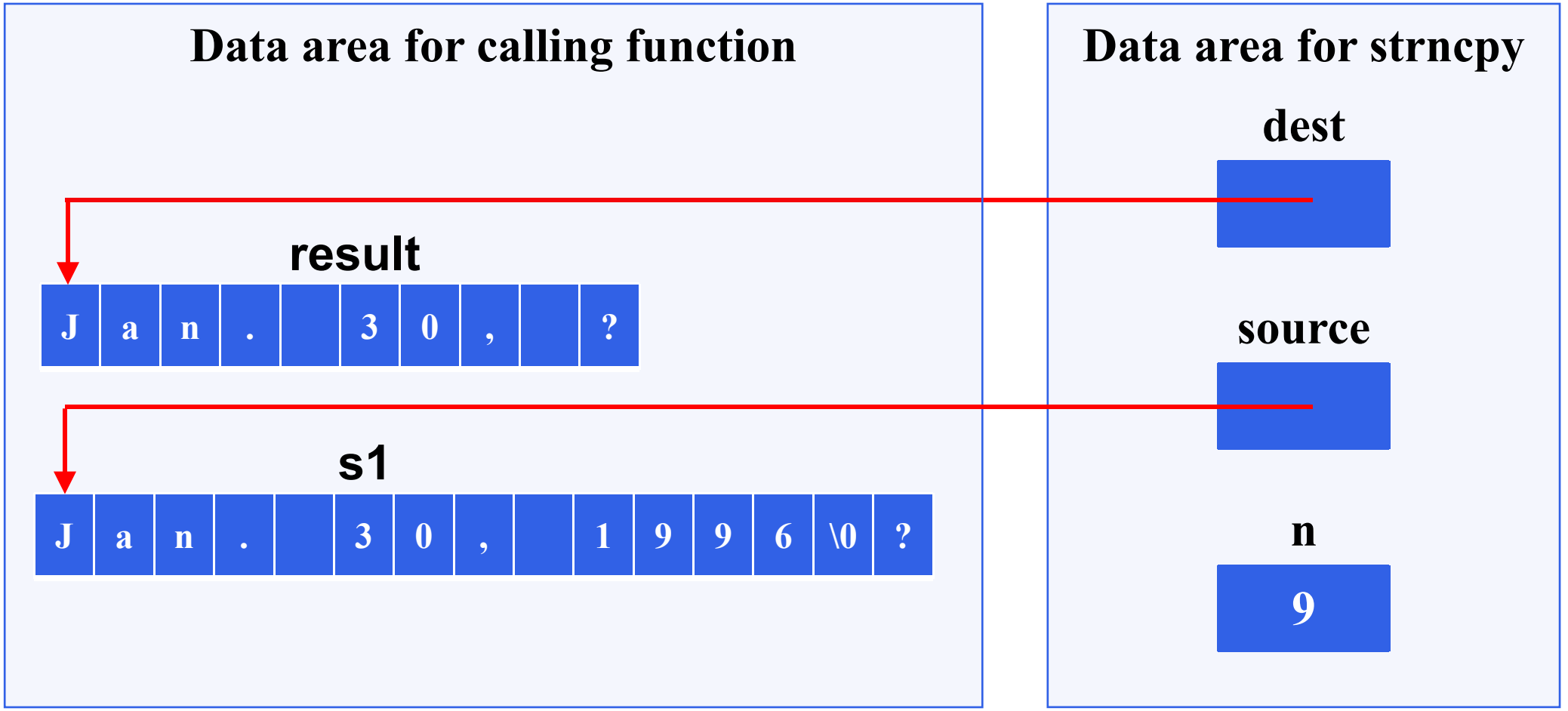
Fangtian Zhong
CSCI 112

Gianforte School of Computing
Norm Asbjornson College of Engineering
E-mail: fangtian.zhong@montana.edu

2024.03.06

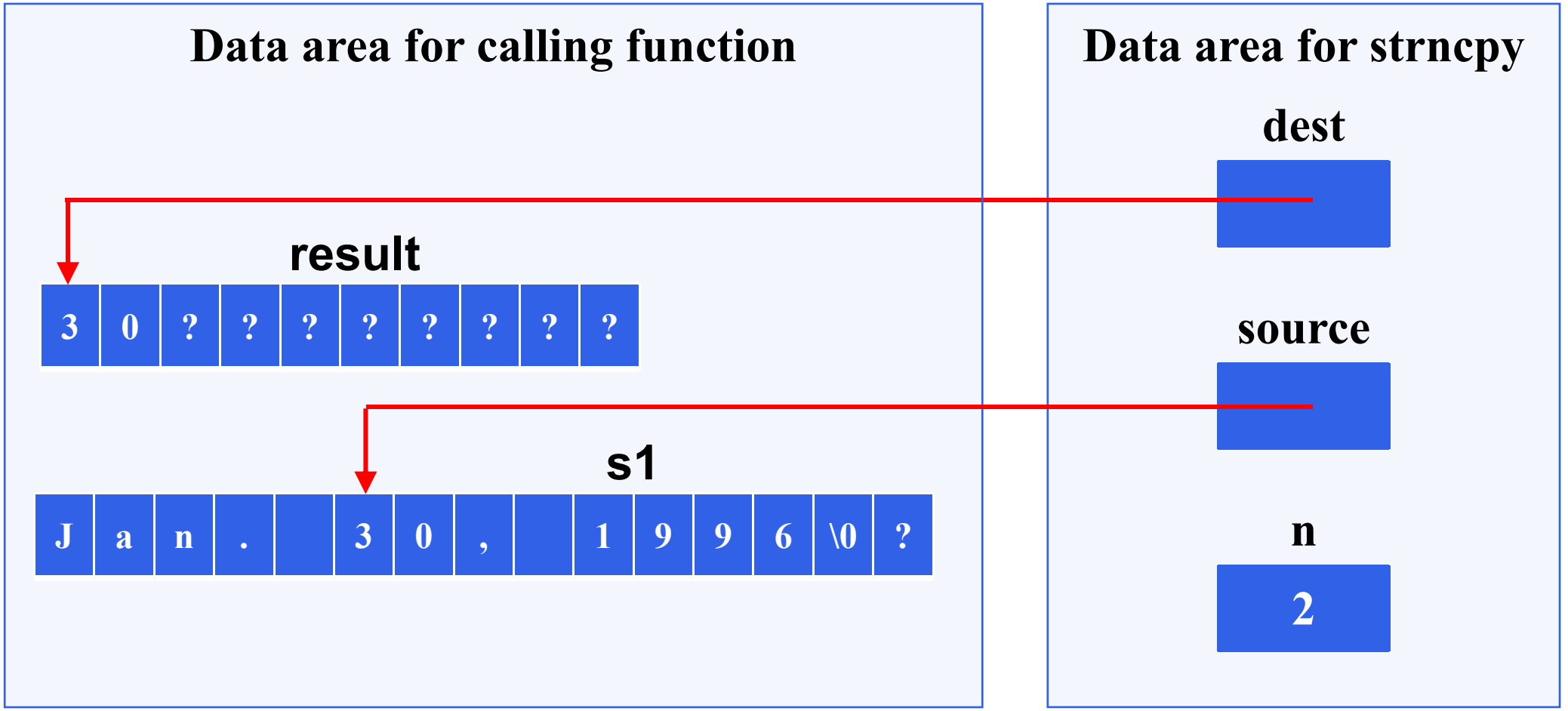
Substrings

Figure Execution of strncpy(result, s1, 9);



Substrings

Figure Execution of strncpy(result, &s1[5], 2);



Substrings

```
char last  [20], first  [20], middle  [20];
char pres[20] = “Adams, John Quincy”;
```

```
strncpy (last, pres, 5);
last[5] = ’\0’;
```

```
strncpy (first, &pres[7], 4);
first[4] = ’\0’;
```

```
strcpy (middle, &pres[12]);
```

J	o	h	n	\0	?	?	?	?	?	?	?	?	?	?	?	?	?	?	?

Buffer Overflow

- more data is stored in an array than its declared size allows
- a very dangerous condition
- unlikely to be flagged as an error by either the compiler or the run-time system

char string[8] = “hello world”;

Concatenation

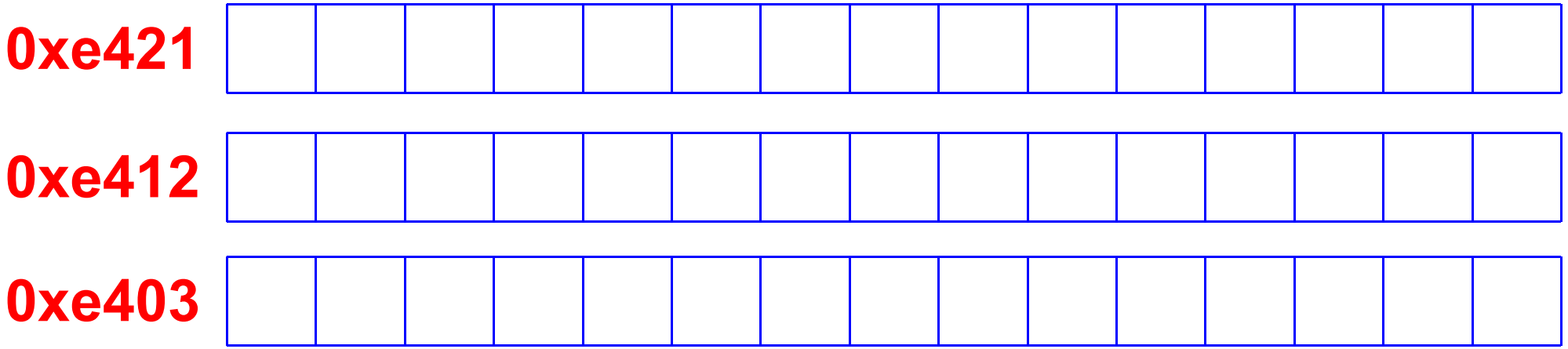
- **strcat**
  - appends source to the end of dest
  - assumes that sufficient space is allocated for the first argument to allow addition of the extra characters
    - s1 = “hello”;
    - strcat(s1, “and more”);

Concatenation

- **strcat**
  - appends up to n characters of source to the end of dest, adding the null character if necessary
  - assumes that sufficient space is allocated for the first argument to allow addition of the extra characters
    - s1 = “hello”;
    - strncat(s1, “and more”, 5);

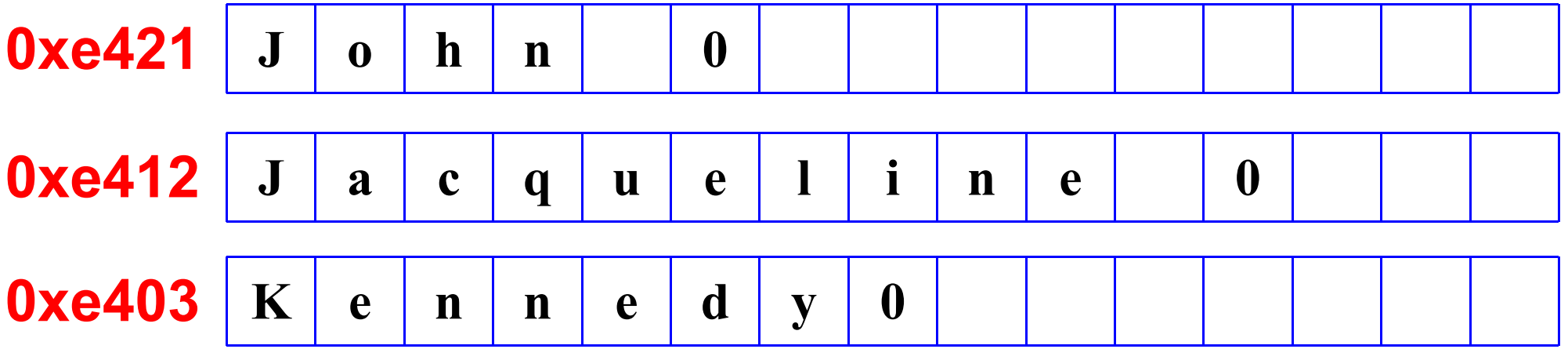
Concatenation

```
char k1[15] = “John “,
        k2[15] = “Jacqueline “,
        last[15] = “Kennedy”;
strcat(k1,last);
strcat(k2,last);
```



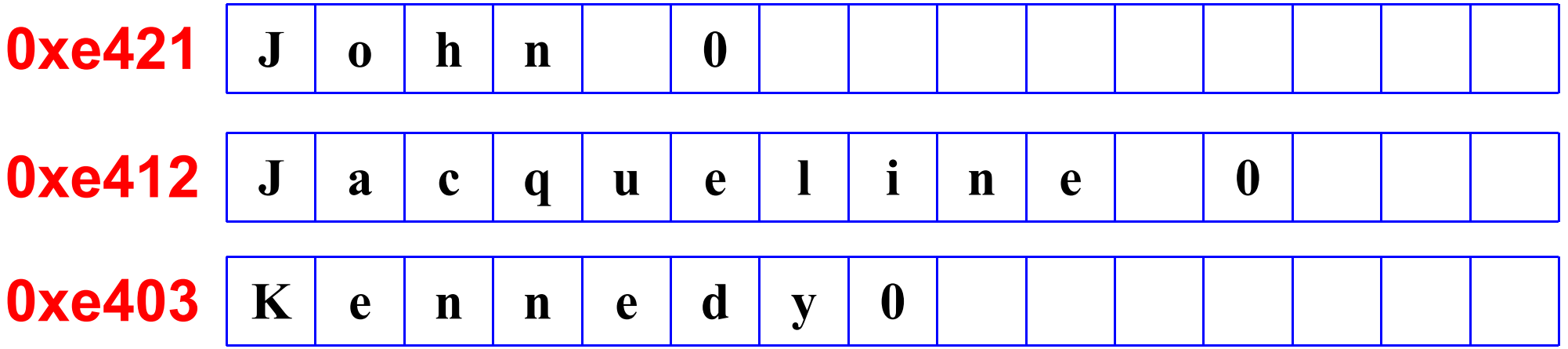
Concatenation

```
char k1[15] = “John “,
        k2[15] = “Jacqueline “,
        last[15] = “Kennedy”;
strcat(k1,last);
strcat(k2,last);
```



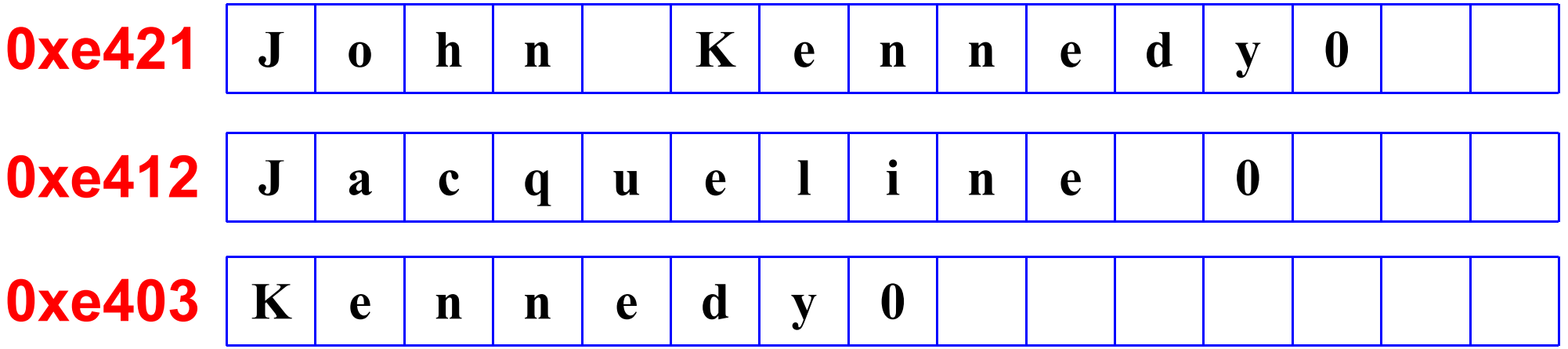
Concatenation

```
char k1[15] = “John “,
     k2[15] = “Jacqueline “,
     last[15] = “Kennedy”;
strcat(k1,last);
strcat(k2,last);
```



Concatenation

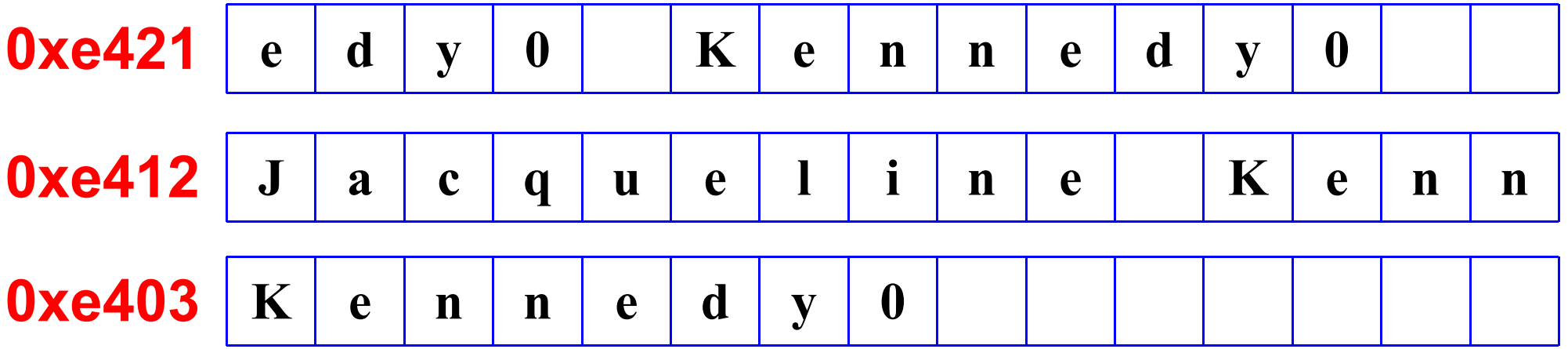
```
char k1[15] = “John “,
        k2[15] = “Jacqueline “,
        last[15] = “Kennedy”;
strcat(k1,last);
strcat(k2,last);
```



Concatenation

```
char k1[15] = “John “,
        k2[15] = “Jacqueline “,
        last[15] = “Kennedy”;
strcat(k1,last);
strcat(k2,last);
```

overflow!



THE END

Fangtian Zhong
CSCI 112

Gianforte School of Computing
Norm Asbjornson College of Engineering
E-mail: fangtian.zhong@montana.edu

2024.03.06