



СЕТИ. БЕЗОПАСНОСТЬ

Урок 38

Стеганография

Алгоритмическая

- Особенности кодирования
- Особенности восприятия
- Особенности контекста

Техническая

- Недокументированные возможности ПО
- Особенности реализаций ПО
- Специальные программные средства

Изображение



Изображение

42	4D E6 04 00 00 00 00	00 00 36 00 00 00 28 00	BM.....6...(. .
	00 00 14 00 00 00 14 00	00 00 01 00 18 00 00 00
	00 00 B0 04 00 00 00 00	00 00 00 00 00 00 00 00	..°.....
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 FF FF FF FF FF FF	FF FF FF FF FF FF 00 00	..AAAAAAAAAAAA..
	00 00 00 00 00 00 00 00	00 00 FF FF FF FF FF FFAAAAAA
	FF FF FF FF FF FF 00 00	00 00 00 00 00 00 00 00	AAAAA.....
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 FF FFAA
	FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00	AAAAAAAAAAAA.....
	00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FFAAAAAAAAAA
	FF FF 00 00 00 00 00 00	00 00 00 00 00 00 00 00	AA.....
	00 00 00 00 00 00 00 00	00 00 FF FF FF FF FF FFAAAAAA
	FF FF FF FF FF FF 00 00	00 00 00 00 00 00 00 00	AAAAA.....
	00 00 FF FF FF FF FF FF	FF FF FF FF FF FF 00 00	..AAAAAAAAAAAA..
	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
	00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FFAAAAAAAAAA
	FF FF 00 00 00 00 00 00	00 00 00 00 00 00 FF FF	AA.....AA
	FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00	AAAAAAAAAAAA.....
	00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FFAAAAAAAAAA
	FF FF 00 00 00 00 00 00	00 00 00 00 00 00 FF FF	AA.....AA
	FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00	AAAAAAAAAAAA.....
	00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FFAAAAAAAAAA



Изображение

42	4D	E6	04	00	00	00	00	00	00	00	00	36	00	00	00	28	00	ВМж.....6...(. .
00	00	14	00	00	00	14	00	00	00	00	00	01	00	18	00	00	00
00	00	B0	04	00	00	00	00	00	00	00	00	00	00	00	00	00	00	..°.....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	..яяяяяяяяяяяя..
00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FFяяяяяя
FF	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	00	яяяяяя.....
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	FFяя
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	яяяяяяяяяя.....
00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FFяяяяяяяяяяяя
FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	яя.....
00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FFяяяяяя
FF	FF	FF	FF	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	00	яяяяяя.....
00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	..яяяяяяяяяяяя..
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FFяяяяяяяяяяяя
FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	яя.....яя
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	яяяяяяяяяя.....
00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FFяяяяяяяяяяяя
FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	00	00	FF	FF	яя.....яя
FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	яяяяяяяяяя.....
00	00	00	00	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FFяяяяяяяяяяяя



TOP SECRET TEXT

54 4F 50 20 53 45 43 52 45 54 20 54 45 58 54 + TOP SECRET TEXT

Изображение

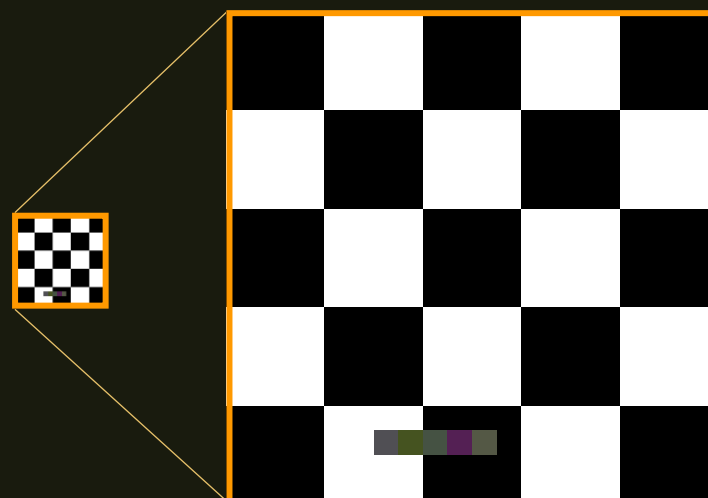
[illegible]

TOP SECRET TEXT

54 4F 50 20 53 45 43 52 45 54 20 54 45 58 54 + TOP SECRET TEXT

Изображение

42 4D E6 04 00 00 00 00	00 00 36 00 00 00 28 00	BM.....6...(.
00 00 14 00 00 14 00	00 00 01 00 18 00 00 00
00 00 B0 04 00 00 00 00	00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00 00 FF FF FF FF FF FF	FF FF FF FF FF FF 00 00
00 00 00 00 00 00 00 00	00 00 FF FF FF FF FF FF
FF FF FF FF FF FF 00 00	00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00	00 00 00 00 00 00 FF FF
FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00
00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FF
FF FF 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00	00 00 FF FF FF FF FF FF
54 4F 50 20 53 45 43 52	45 54 20 54 45 58 54 00	TOP SECRET TEXT.
00 00 FF FF FF FF FF FF	FF FF FF FF FF FF 00 00
00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FF
FF FF 00 00 00 00 00 00	00 00 00 00 00 00 FF FF
FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00
00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FF
FF FF 00 00 00 00 00 00	00 00 00 00 00 00 FF FF
FF FF FF FF FF FF FF FF	FF FF 00 00 00 00 00 00
00 00 00 00 00 00 FF FF	FF FF FF FF FF FF FF FF



LSB

Менее простой метод стеганографии в изображениях

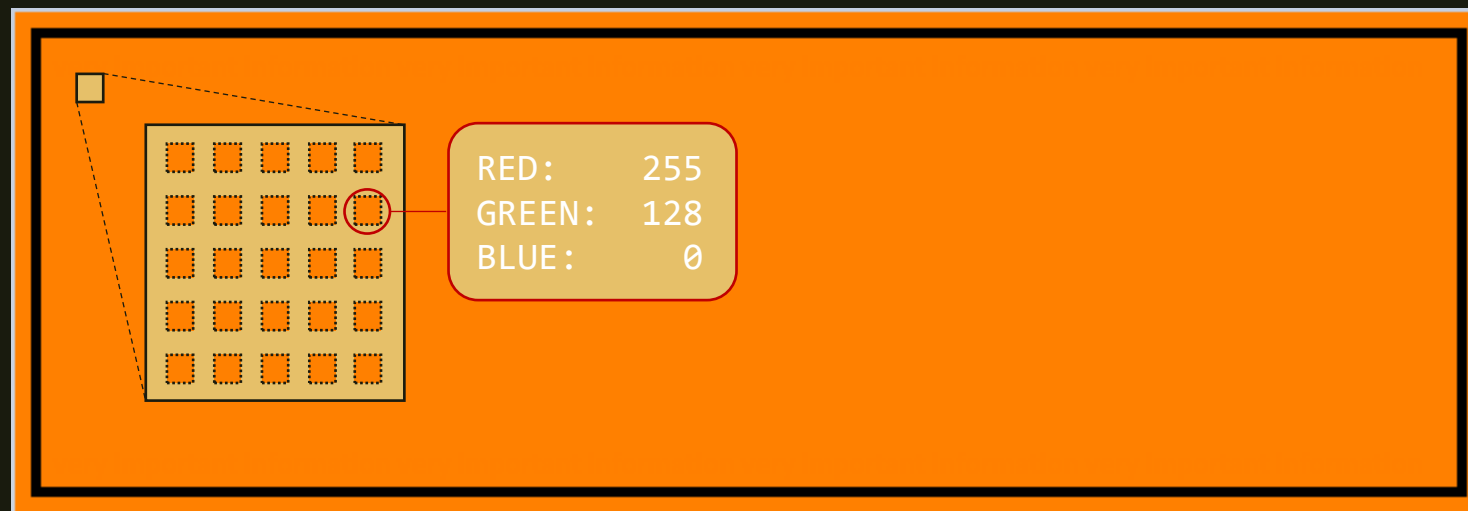
Изображение



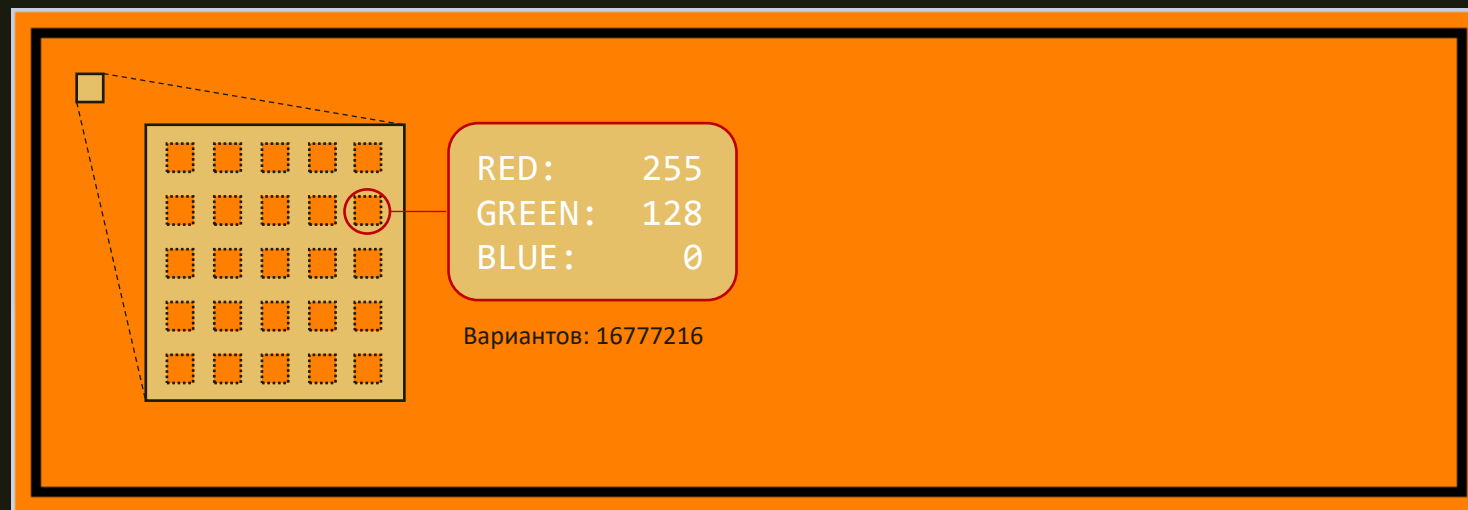
Пиксели



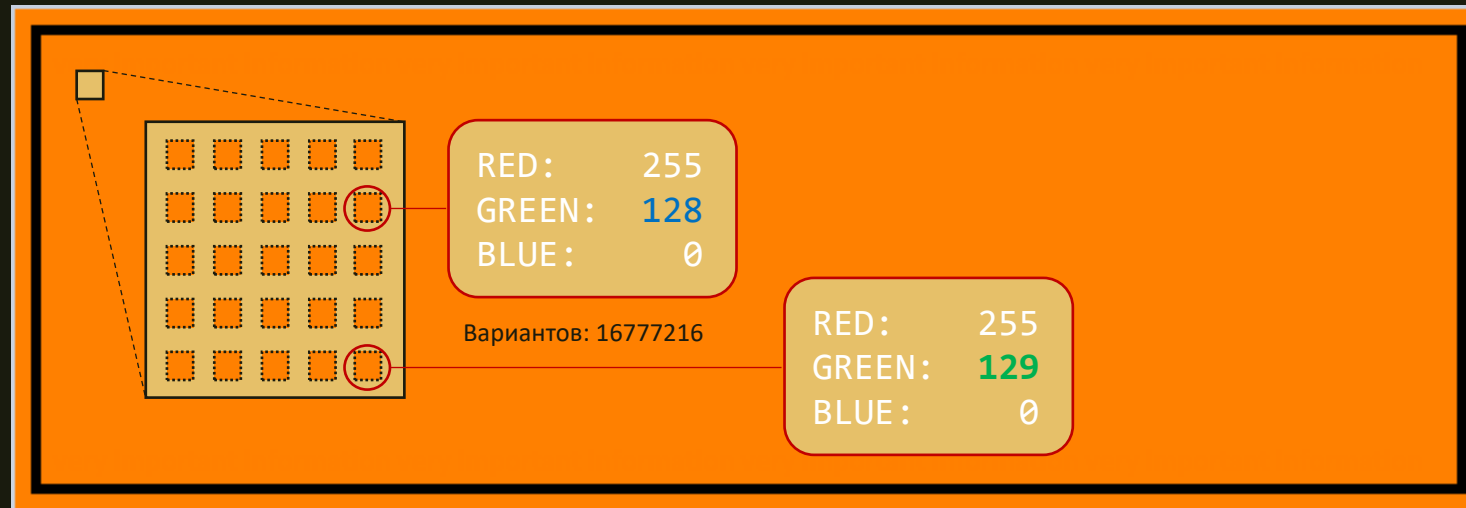
Числа



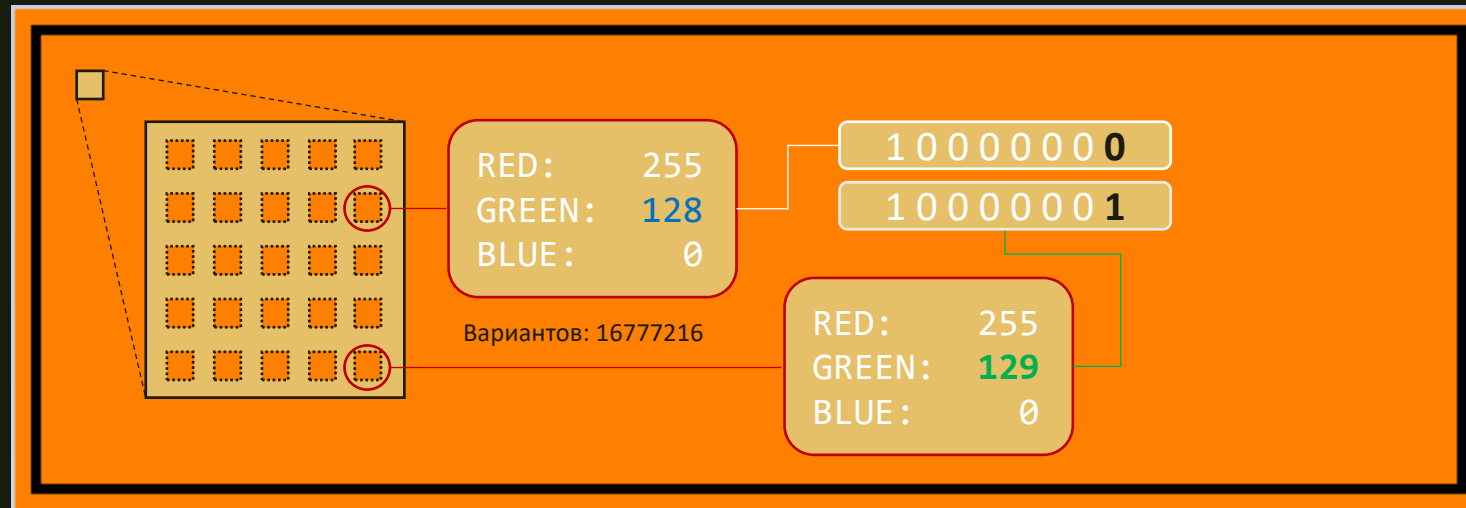
Числа



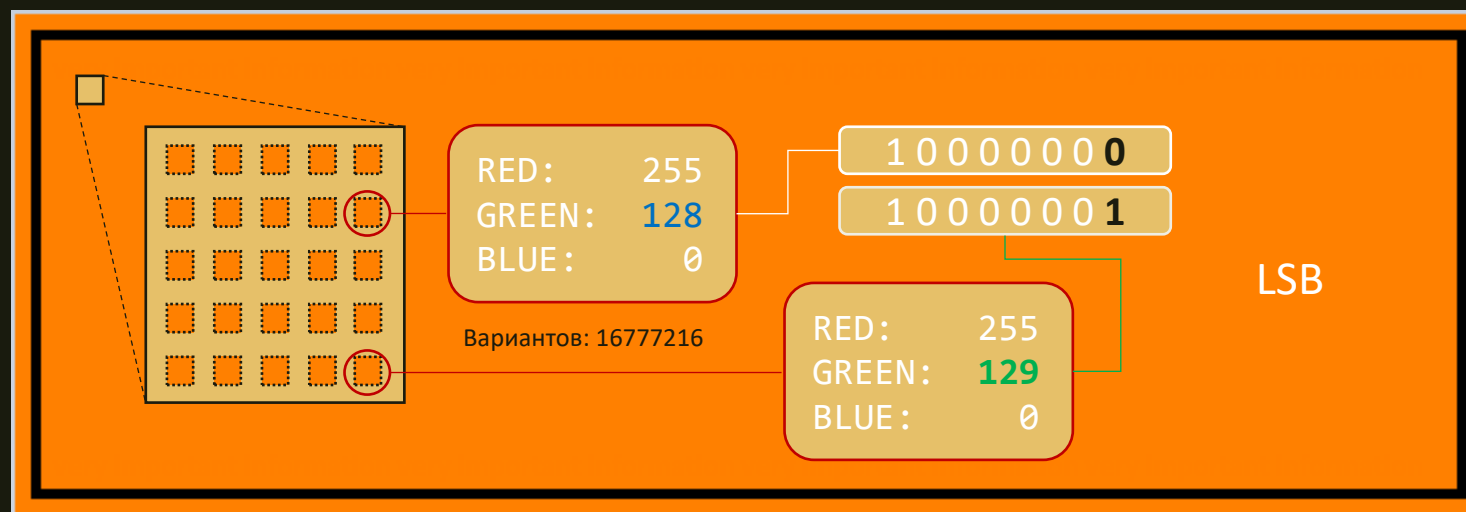
Разные числа



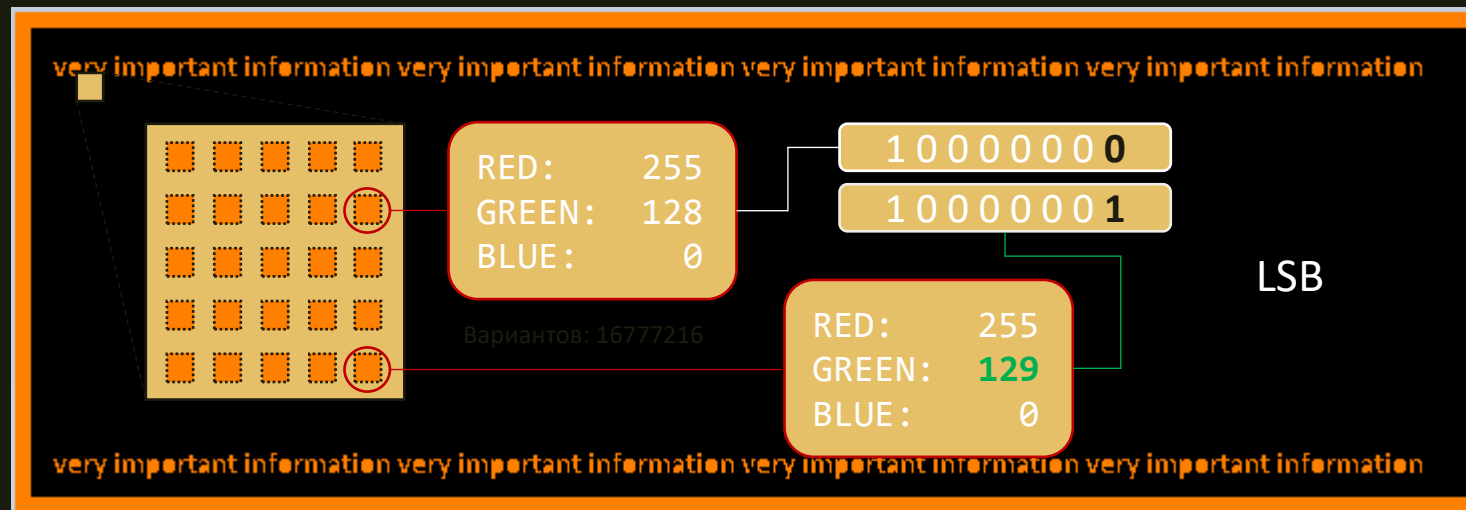
Минимальные отличия



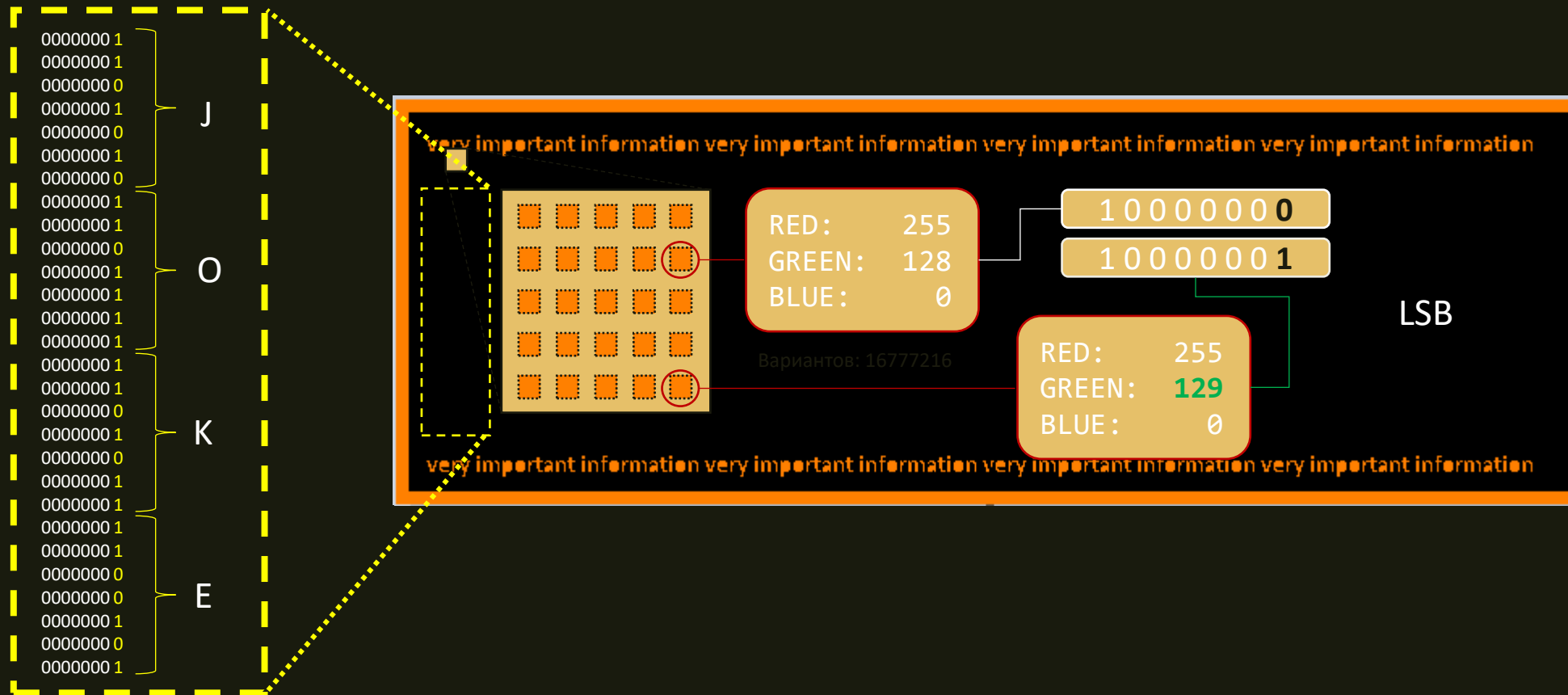
Least Significant Bit



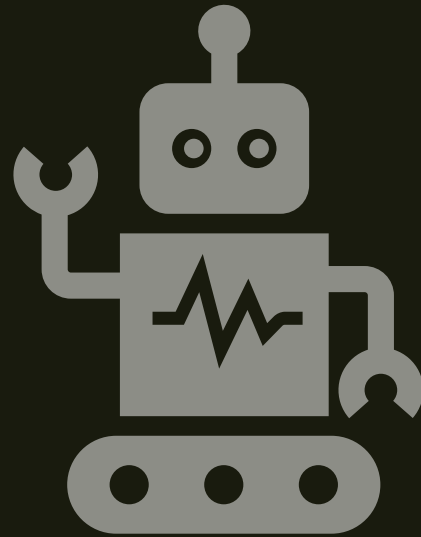
Скрытая информация



Скрытая информация



Практика



ADS

Совершенно “случайная” технология

Жесткий диск



Файл



Жесткий диск



Файл



имя / путь

метаданные

данные

Жесткий диск



boot



head



i-node

кластеры

Файл

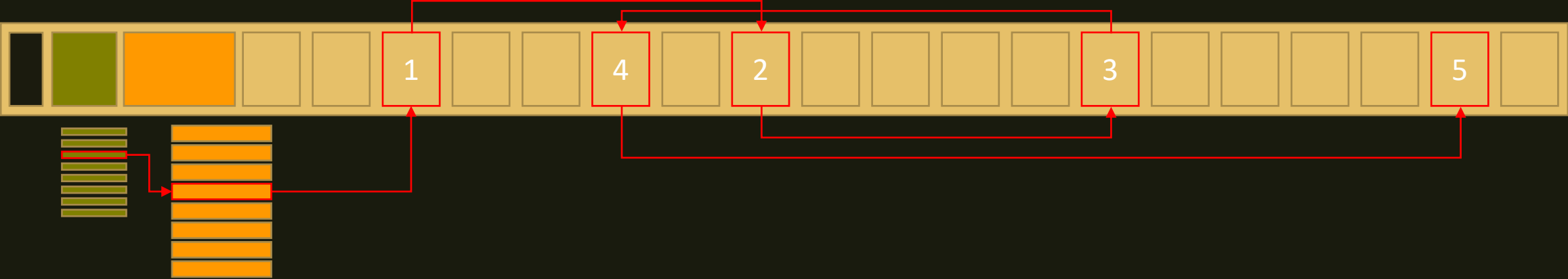


имя / путь

метаданные

данные

Жесткий диск

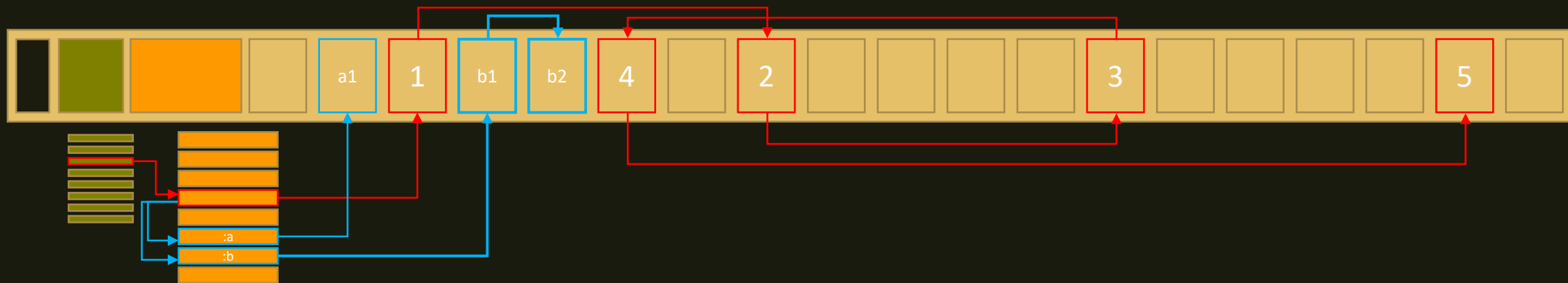


Файл



имя / путь
метаданные
данные

Жесткий диск



Файл



имя / путь

метаданные

данные

ADS

Вывод:

```
echo text
```

Вывод в файл:

```
echo text > file.txt
```

Вывод в поток:

```
echo text > file.txt:potok1
```

```
echo text > file.txt:potok2
```

Чтение из файла:

```
more file.txt
```

Чтение из потока:

```
more < file.txt:potok1
```

```
more < file.txt:potok2
```

Файлы в папке:

```
dir /B
```

Вывести все файлы в папке:

```
for /f %i in ('dir /B') do more %i
```

Создать серию файлов:

```
for /l %i in (1,1,10) do echo hello>file%i.txt
```

Копирование серии файлов в один:

```
for /l %i in (1,1,10) do echo hello%i>>file11.txt
```

Копирование из потока:

```
more < file.txt:potok1 > new_file.txt
```

Вывести файл по строкам:

```
for /f %i in (file11.txt) do echo %i
```