# Исследование возможности использования подмены библиотеки для реализация палитры команд

Студент: Польшаков Д.В.
Научный руководитель: Чернышов М.К.

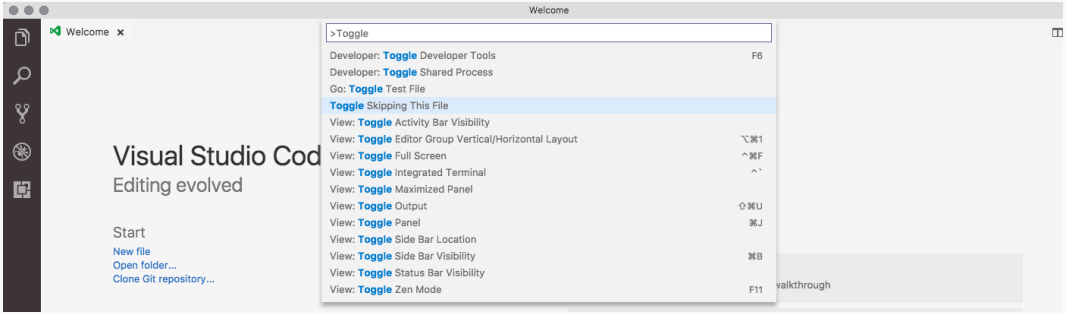
2020

ВГУ

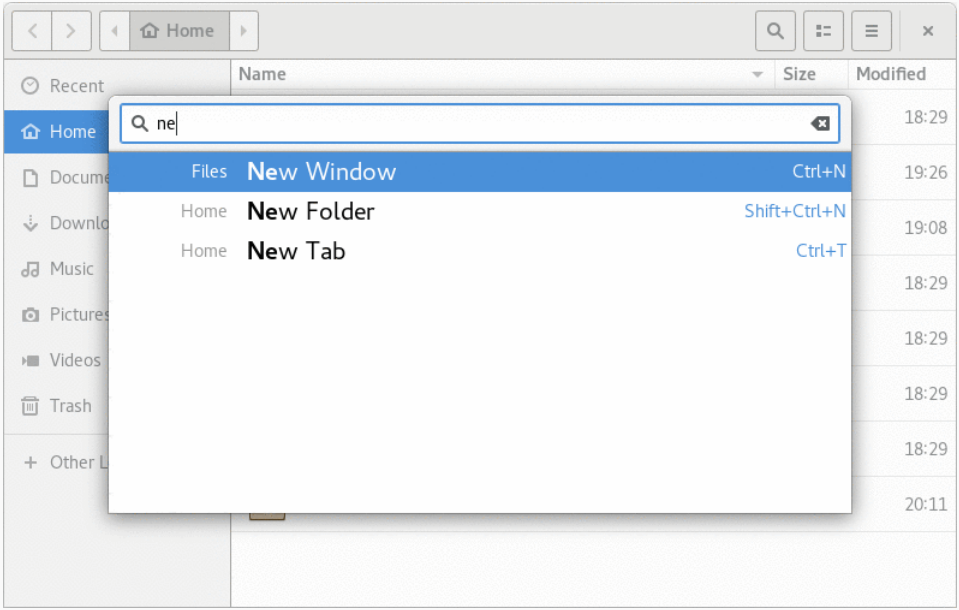
# Палитра команд

Это специальное окно в интерфейсе приложения, где отображаются все доступные функции. Иногда рядом с описанием функции отображается горячая клавиша для её активации.

# Палитра команд в VS Code



# Палитра команд в Plotinus



**Qt** — кроссплатформенный фреймворк для разработки программного обеспечения на языке программирования C++. Включает в себя в т.ч. классы для разработки графического интерфейса.

# Добавление логики в приложение

**Способы добавления дополнительной логики в приложение**

- добавление функции на этапе сборки приложения
- добавление функции в момент выполнения программы
  - с помощью загрузка плагинов
  - с помощью подмены библиотек

# Постановка задачи

Разработать набор программ, которые в комплексе будут решать следующие задачи:

- запускать целевые приложения в специальном окружении
- собирать информацию о существующих элементах графического приложения
- сохранять информацию о всех запущенных приложениях
- отображать пользователю окно для поиска и выбора элемента
- активировать выбранный пользователем элемент

# Постановка задачи

Набор программ должен быть реализован в виде следующих элементов:

1. Библиотека для внедрения и сбора информации в конкретном приложении.
2. Приложение для сохранения информации, полученой из нескольких приложения с библиотекой из п.**??**.
3. Графический интерфейс для запуска приложений и отображения окна палитры комманд.

# Генерация кода

Искажение имен (name mangling):

- `QCheckBox::QCheckBox(const QString&, QWidget*)`
- `_ZN9QCheckBoxC1ERK7QStringP7QWidget_f`
- `void QAbstractButton::setText(const QString&)`
- `_ZN15QAbstractButton7setTextERK7QString_f`

# Генерация кода

Однотипный код

```
typedef bool *func_f(int a, char* s);
static func_f real_func = 0;

bool func(int a, char* s)
{
    if (!real_func)
        real_func = (func_f)dlsym(RTLD_NEXT, "func");

    if (initInject())
        handle_for_func(a, s); // to change

    return real_func(a, s);
}
```

# Протокол

```
<команда> ::= <имя-команды> <параметры-команды>
<имя-команды> ::= <строка>
<строка> ::= <длина-строки> <идентификатор>
<длина-строки> ::= uint32_t
<идентификатор> ::= "newApp"
                ::= "setWidgetText"
                ::= "remove"
                ::= "activated"
                ::= "setWidgetWindow"
                ::= "activate"
```

# Интерфейс

Сочетания клавиш

- Запуск: Ctrl + Shift + D
- Палитра: Ctrl + Shift + S

# Интерфейс

**Запуск приложений**

**Палитра команд**

# Заключение

- Реализована библиотека, для перехвата событий
- Реализован вспомогательный генератор для расширения библиотеки
- Разработано приложение для внедрения библиотеки и отображения палитры команд

# Исследование возможности использования подмены библиотеки для реализация палитры команд

Студент: Польшаков Д.В.
Научный руководитель: Чернышов М.К.

2020

ВГУ