

Исследование возможности использования подмены библиотеки для реализация палитры команд

Студент: Польшаков Д.В.

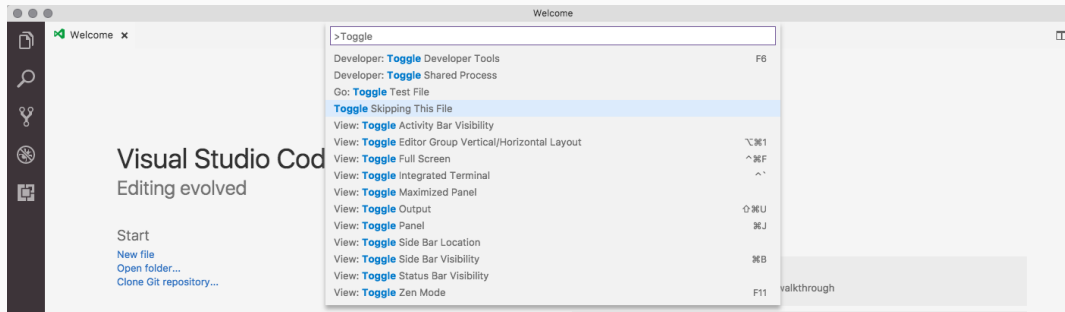
Научный руководитель: Чернышов М.К.

2020

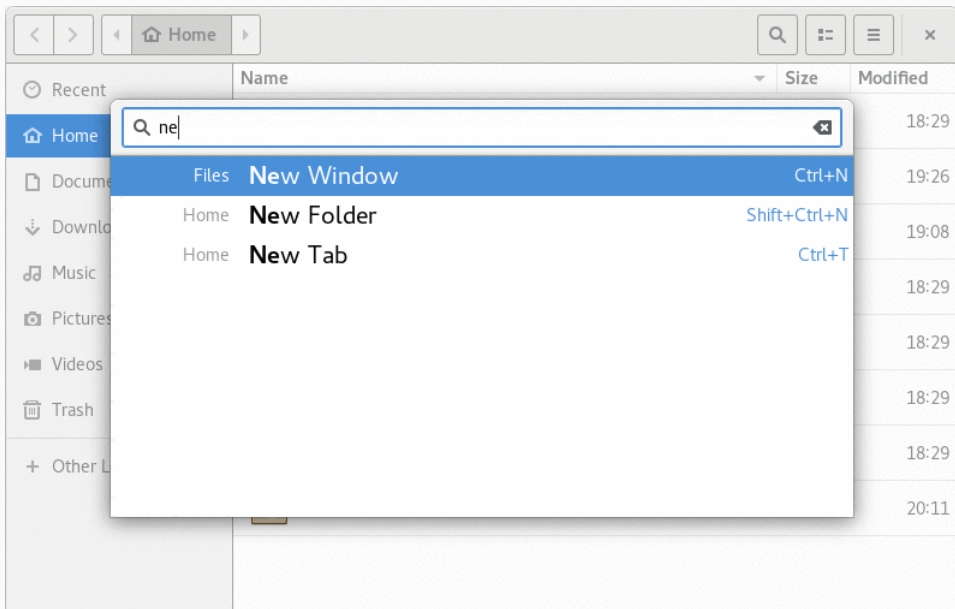
ВГУ

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.

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

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

Набор программ должен быть реализован в виде следующих элементов:

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

Искажение имен (name mangling):

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

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");

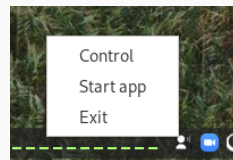
    if (initInject())
        handle_for_func(a, s); // to change

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

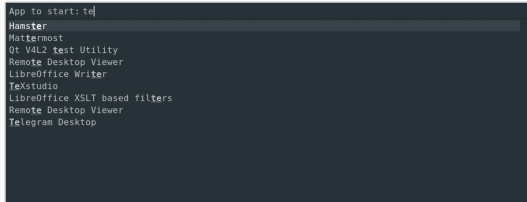
```
<команда> ::= <имя-команды> <параметры-команды>
<имя-команды> ::= <строка>
<строка> ::= <длина-строки> <идентификатор>
<длина-строки> ::= uint32_t
<идентификатор> ::= "newApp"
                  ::= "setWidgetText"
                  ::= "remove"
                  ::= "activated"
                 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

Сочетания клавиш

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



Запуск приложений



A screenshot of a terminal window with a dark background. At the top, the prompt 'App to start: te|' is visible. Below it, a list of application names is displayed, with 'Hamster' highlighted by a horizontal bar. The list includes: Hamster, Mattermost, Qt V4L2 test Utility, Remote Desktop Viewer, LibreOffice Writer, TeXstudio, LibreOffice XSLT based filters, Remote Desktop Viewer, and Telegram Desktop.

```
App to start: te|
Hamster
Mattermost
Qt V4L2 test Utility
Remote Desktop Viewer
LibreOffice Writer
TeXstudio
LibreOffice XSLT based filters
Remote Desktop Viewer
Telegram Desktop
```

Палитра команд



A screenshot of a command palette interface with a dark background. At the top, the prompt ': pr|' is visible. Below it, a list of command names is displayed, with 'Properties' highlighted by a horizontal bar. The list includes: Properties, Preferences, and Sort by Progress.

```
: pr|
Properties
Preferences
Sort by Progress
```

- 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