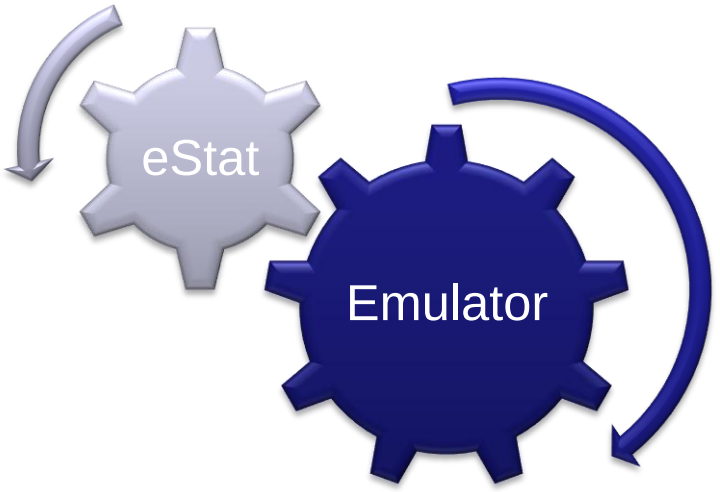
Статический анализ бинарных файлов eStat

Участники:
Казенюк Сергей
Коклюев Сергей
Котельников Роман
Тураев Марат

Куратор:
Сиднев Алексей

Актуальность

- Изучение дизассемблера
- Получение набора инструкций, который необходимо эмулировать (утилит с необходимой функциональностью найдено не было)
- Оценка эффективности компиляции (использования набора инструкций).



Постановка задачи

- Разработать программу, позволяющую выполнять статический анализ исполняемых файлов:
  - выводить тип и количество инструкций, содержащихся в бинарном файле;
  - выполнять группировку инструкций по заданному шаблону.

Обзор дизассемблеров

	Disit	BeaEngine	Xde101	diStorm64
Частота обновления	-	+	+	+
Набор инструкций	-	+	-	+
Выдаваемые данные	+	+	-	+
Удобство использования	+	-	-	+

Дизассемблер diStorm64

Структура на выходе:

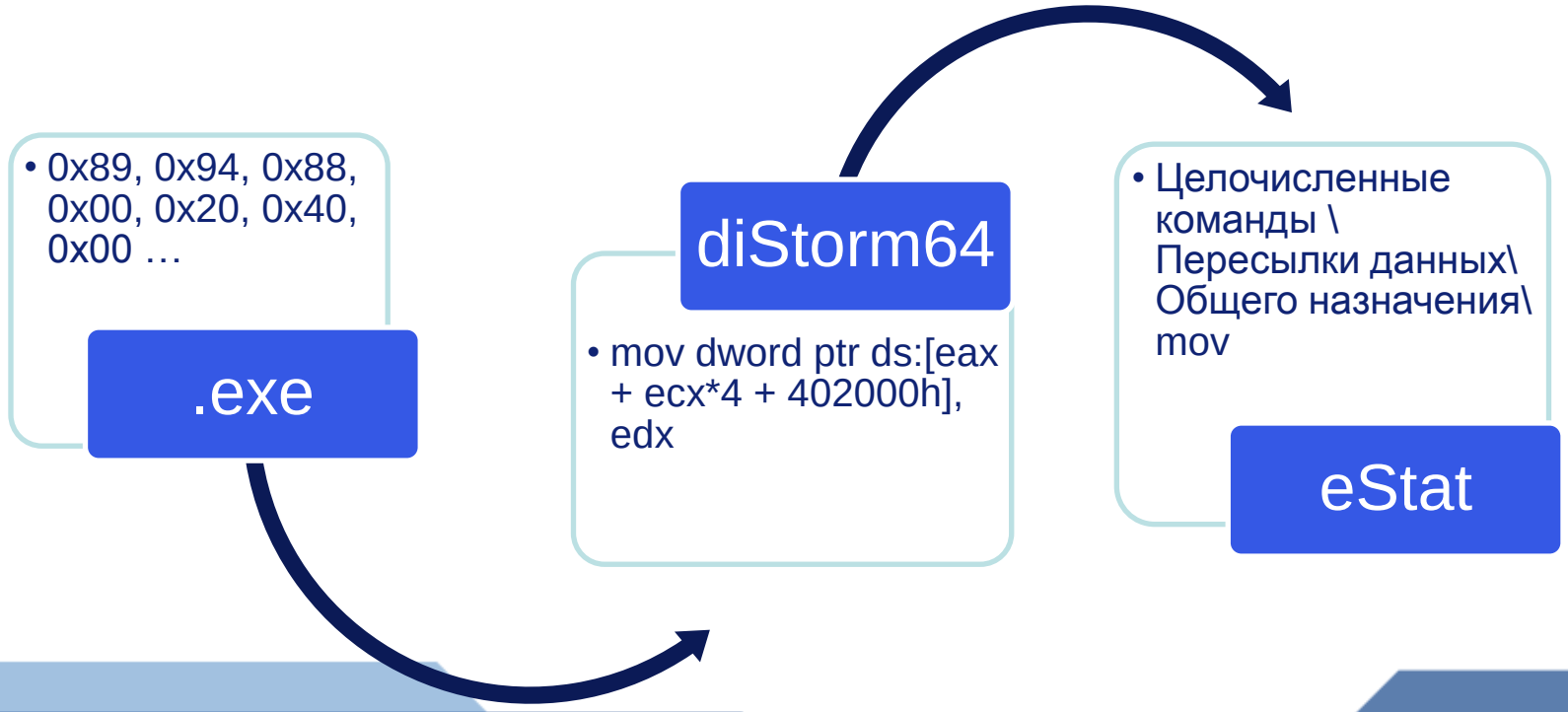
- Сдвиг инструкции по файлу;
- Размер инструкции;
- Код инструкции;
- Текстовое представление инструкции.

Поддерживаемые инструкции:

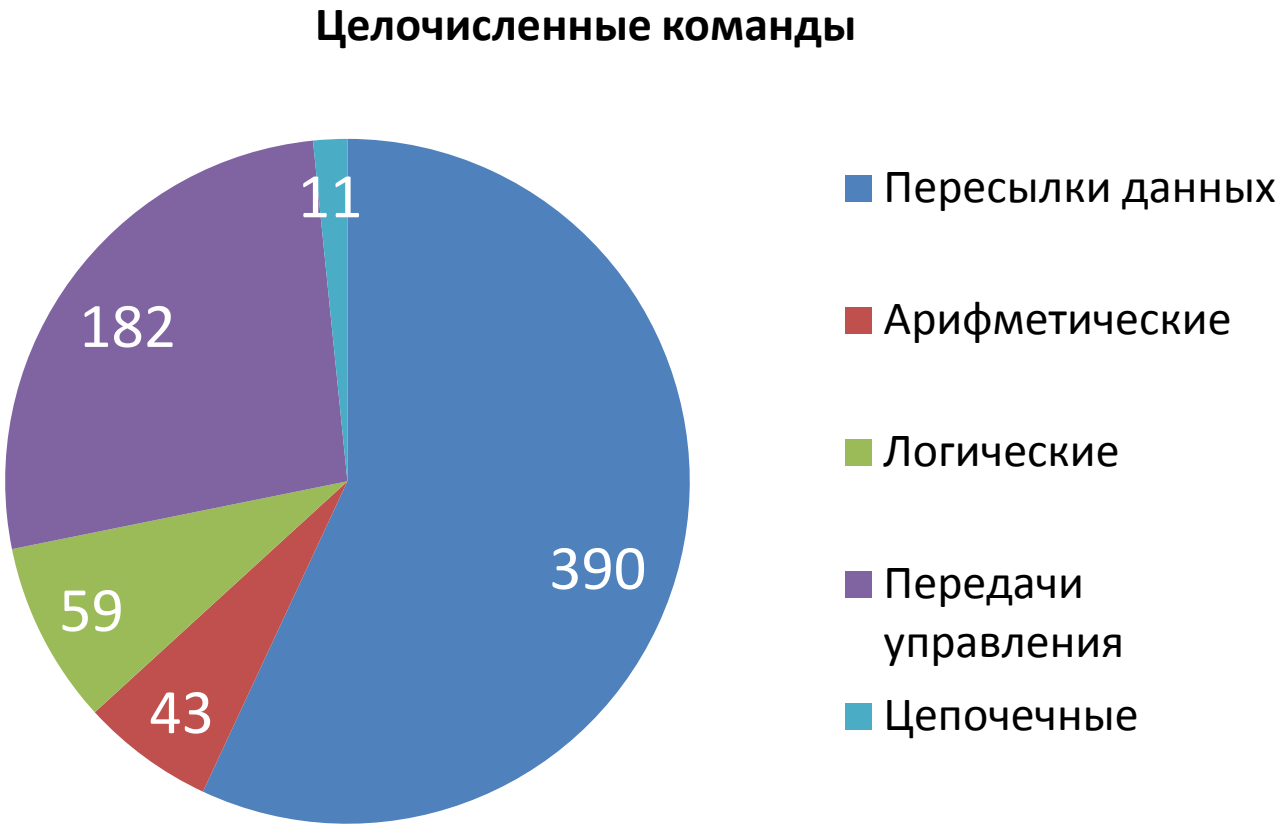
- FPU
- MMX
- SSE, SSE2, SSE3, SSSE3, SSE4
- 3DNow!
- VMX
- AMD's SVM

Алгоритм работы

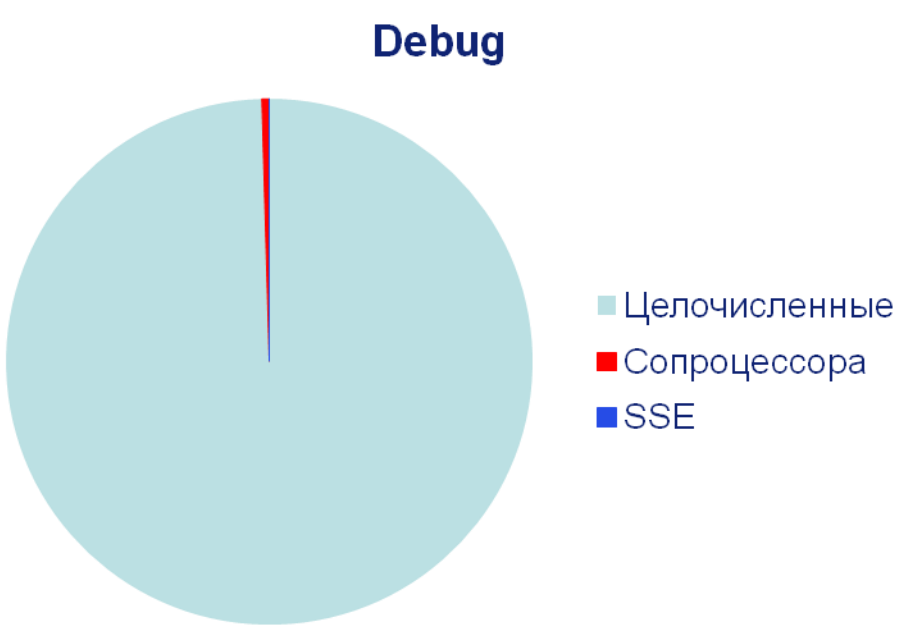
- Исполняемый модуль разбирается библиотекой diStorm64
- С помощью PE заголовка получаем местоположение сегмента кода;
- Полученные данные анализируются и выдаются в требуемом виде



Примеры анализа

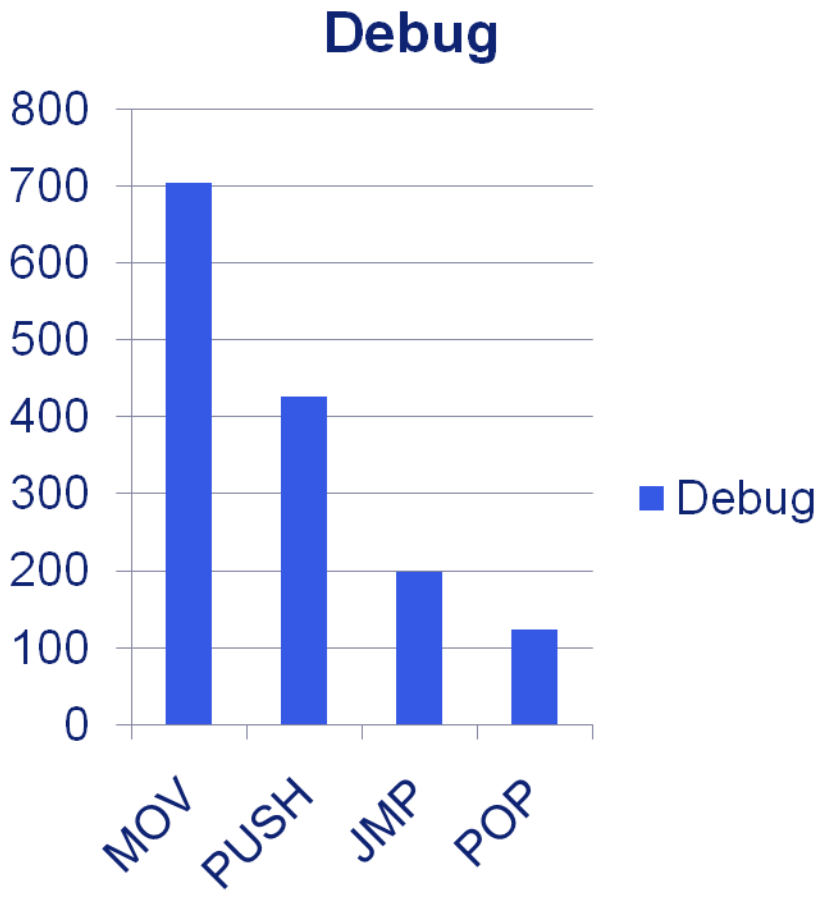


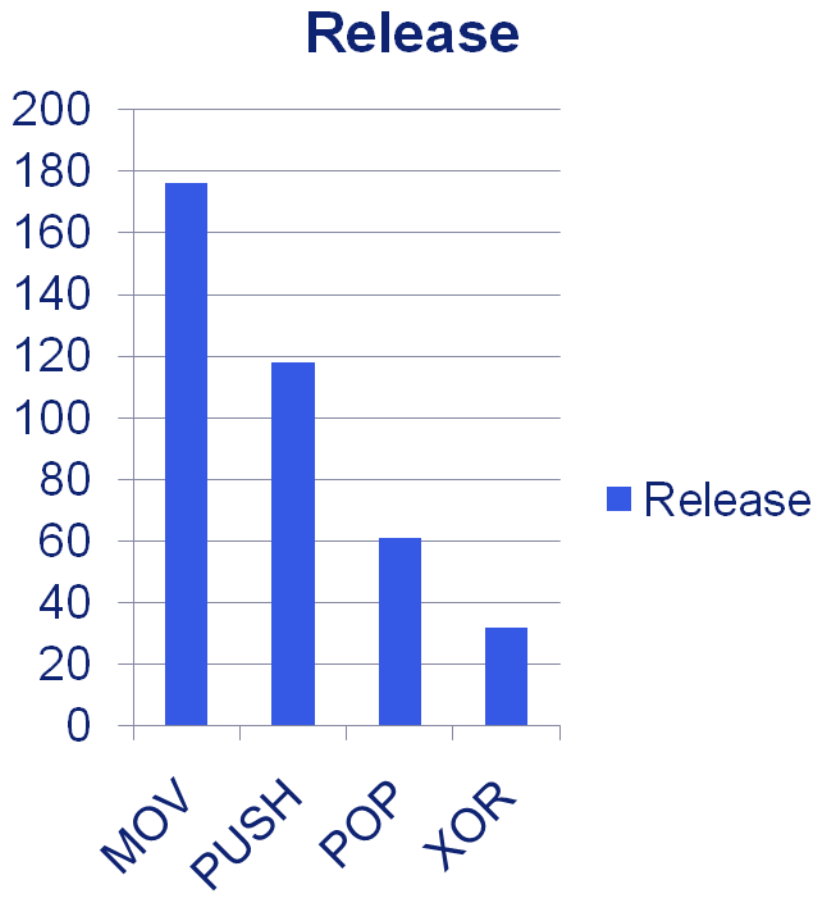
Примеры анализа





Примеры анализа





Замечания

- Защищённые приложения (Software Compress 1.2, Advanced Shell for UPX 1.25, Stealth PE 2.11)
- Поддерживает работу с dll

Результаты

- Разработано приложение, выполняющее статический анализ исполняемого модуля:
  - позволяет выводить тип и количество инструкций, содержащихся в бинарном файле;
  - позволяет выполнять группировку инструкций по заданному шаблону (“В. Юров. Ассемблер”).
- Внешние библиотеки:
  - дизассемблирование реализовано с помощью библиотеки diStorm64;
  - интерфейс реализован с помощью библиотеки разбора аргументов командной строки TCLAP.

Планы

- Дальнейшая разработка эмулятора
- В Сочи в 2014

Вопросы

???