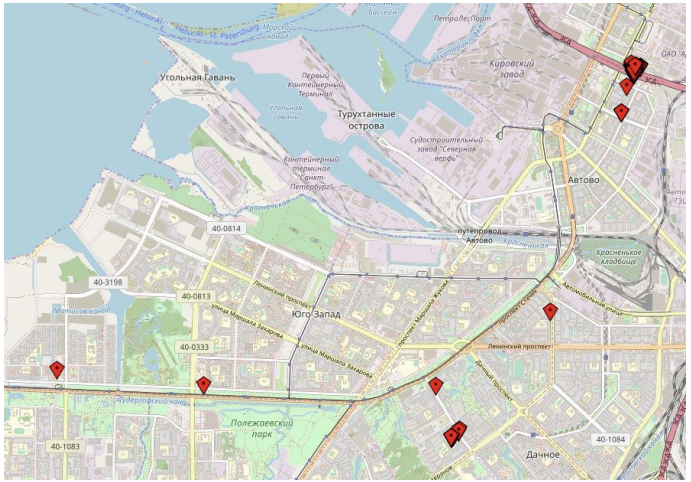
Исследование уязвимости iOS tfp0 для применения в криминалистическом анализе

Виноградов Михаил Викторович, 441 группа

Научный руководитель: к. т. н., доц. Литвинов Ю. В.
Научный консультант: рук. отд. раз. ПО ООО “Белкасофт” Тимофеев Н. М.
Рецензент: специалист лаборатории компьютерной криминалистики и анализа вредоносного кода ООО “Группа АйБи” Михайлов И. Ю.

Введение

- Цифровая криминалистика
- Особый интерес у криминалистов вызывает анализ мобильных устройств компании Apple: iPhone и iPad
- iOS – хорошо защищенная система
- Скрытые геолокационные данные



Цель

Целью работы является разработка программы для создания образа файловой системы устройств на операционной системе iOS и внедрение ее в коммерческий продукт Belkasoft Evidence Center.

Задачи

- Исследовать способы получения данных из мобильного устройства
- Исследовать суть уязвимости «tfp0» и возможность применения данной уязвимости для получения доступа к данным на мобильном устройстве
- Реализовать приложение-прототип для снятия образа и внедрить его в Belkasoft Evidence Center
- Провести апробацию полученного результата

Основные виды извлечения данных с мобильных устройств

- Снятие логического образа – резервная копия через программу iTunes
- Снятие физического образа – полный побитовый образ памяти
- Снятие полного логического образа – копия содержимого файловой системы

Уязвимость tfp0

- В OS X task_for_pid – это функция, которая позволяет процессу получать ссылку на сегмент виртуальной памяти другого процесса
- 0 – идентификатор процесса ядра
- tfp0 – task_for_pid 0

Этапы Jailbreak

- Получение доступа на чтение и запись к сегменту виртуальной памяти ядра
- Получение root доступа
- Обход песочницы
- Обход AppleMobileFileIntegrity
- Установкой утилит tar, ssh, dpkg и т. д. по пути «/var/containers/Bundle/»
- Выставление параметра «com.apple.private.security.container-required» у утилит со значением false

Подключение к устройству

- 8119 – произвольный свободный порт на компьютере
- 27015 – порт AppleMobileDeviceService, который отвечает за распознавание устройств iPhone, iPad и iPod touch в программе iTunes
- 22 – порт SSH

Создание образа

- Установка SSH соединения
- Перенаправление вызова “tar -cf - /” на локальный компьютер

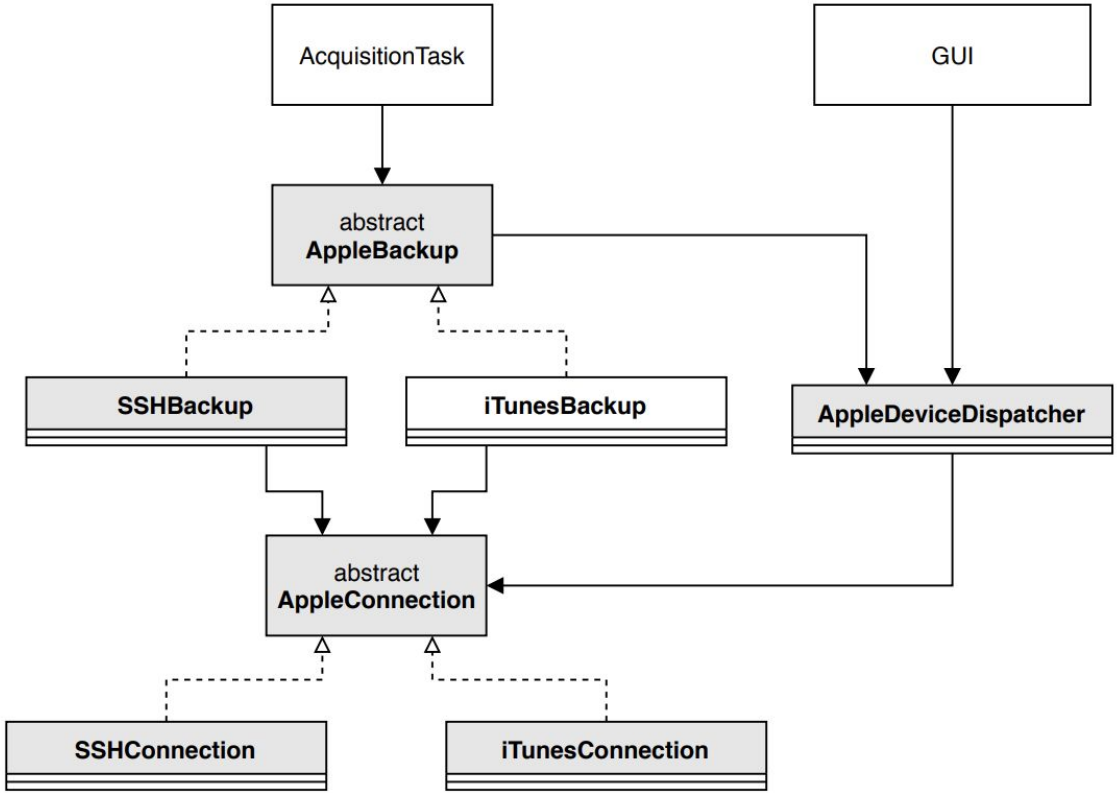
Анализ целесообразности сжатия образа

	lz4	**gzip**	**Без сжатия**
Время, мин	14	27	6,5
Скорость, Мбайт/с	13	3	27,6
Размер, Мбайт	6270	5007	10800

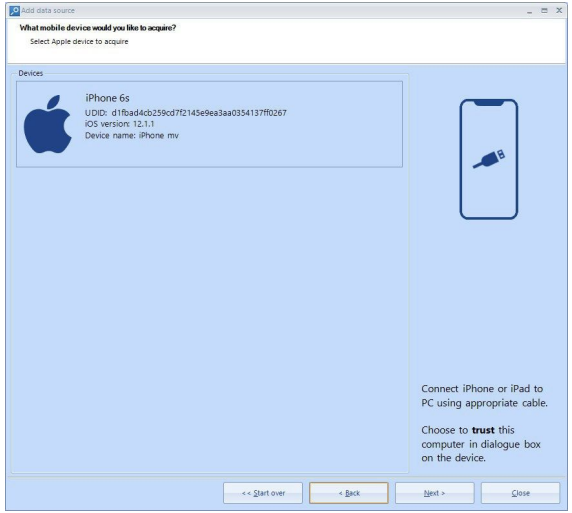
Отключение автоблокировки

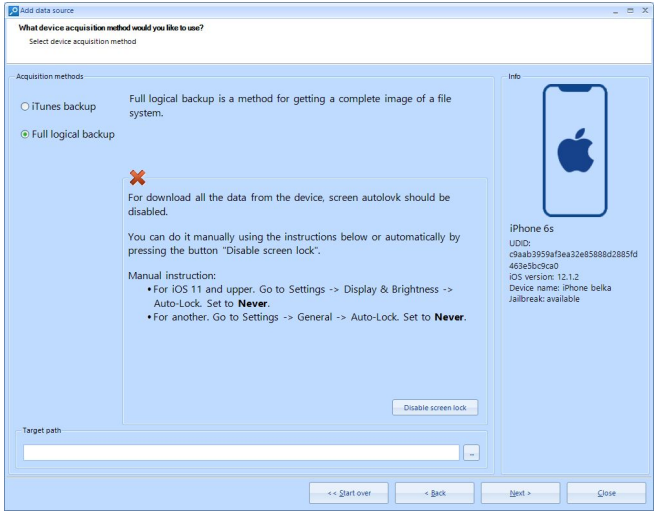
- Метод агента
- Создание утилиты командной строки на языке Objective-C
- Схема снятия автоблокировки экрана:
  - Подключение по SSH
  - Утилита загружается по SSH в папку /usr/bin
  - Запуск утилиты
  - Удаление утилиты с устройства

Интеграция в Belkasoft Evidence Center



Интеграция в Belkasoft Evidence Center





Сравнение логического и полного логического образов

Приложение	Логический образ	Полный логический образ
Facebook, кол. сообщений	0	45
Telegram, кол. сообщений	0	167
WeChat, кол. сообщений	0	80
WhatsApp, кол. сообщений	10	10
Safari, кол. кэшей и ссылок	173	6266

Результаты

- Исследованы способы получения данных из мобильного устройства
- Исследована суть уязвимости «tfp0» и возможность применения данной уязвимости для получения доступа к данным на мобильном устройстве
- Реализовано приложение-прототип для снятия образа и внедрено в Belkasoft Evidence Center
- Проведена апробация