Министерство образования и науки

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Факультет инфокоммуникационных технологий

Отчет

по лабораторной работе № 3

**Аудит защищенности беспроводных Wi-Fi сетей передачи данных. Аудит WPA/WPA2 протоколов Wi-Fi сетей передачи данных с помощью OC Kali Linux. Утилита Aircrack-ng**

по дисциплине «Информационная безопасность в инфокоммуникационных системах»

**Выполнил: студент группы K4220**

**Кислюк Игорь Витальевич**

**Проверил: к.т.н., доцент И.В. Ананченко**

Санкт-Петербург

2018

## Задание.

* Выполнить настройку беспроводной точки доступа для Wi-Fi сети заданной конфигурации;
* Выполнить настройку компьютера для работы с беспроводной сетью;
* Выполнить операцию подключения к сети. Убедиться в работоспособности сети. Дать оценку защищенности беспроводной сети, рекомендации по ее усилению. Для аудита использовать wifite, aircrack-ng, допускается дополнительно использовать другие средства аудита по выбору обучающегося. Предоставить полученный в ходе выполнения лабораторной работы cap-файл, содержащий перехваченное рукопожатие (хендшейк)

## Индивидуальное задание.

* номер 10;
* Тип шифрования: WPA (WPA2). SSID: var10. Ключ подключения: abdominohysterotomy

## Ход работы

Выполним настройку беспроводной сети.

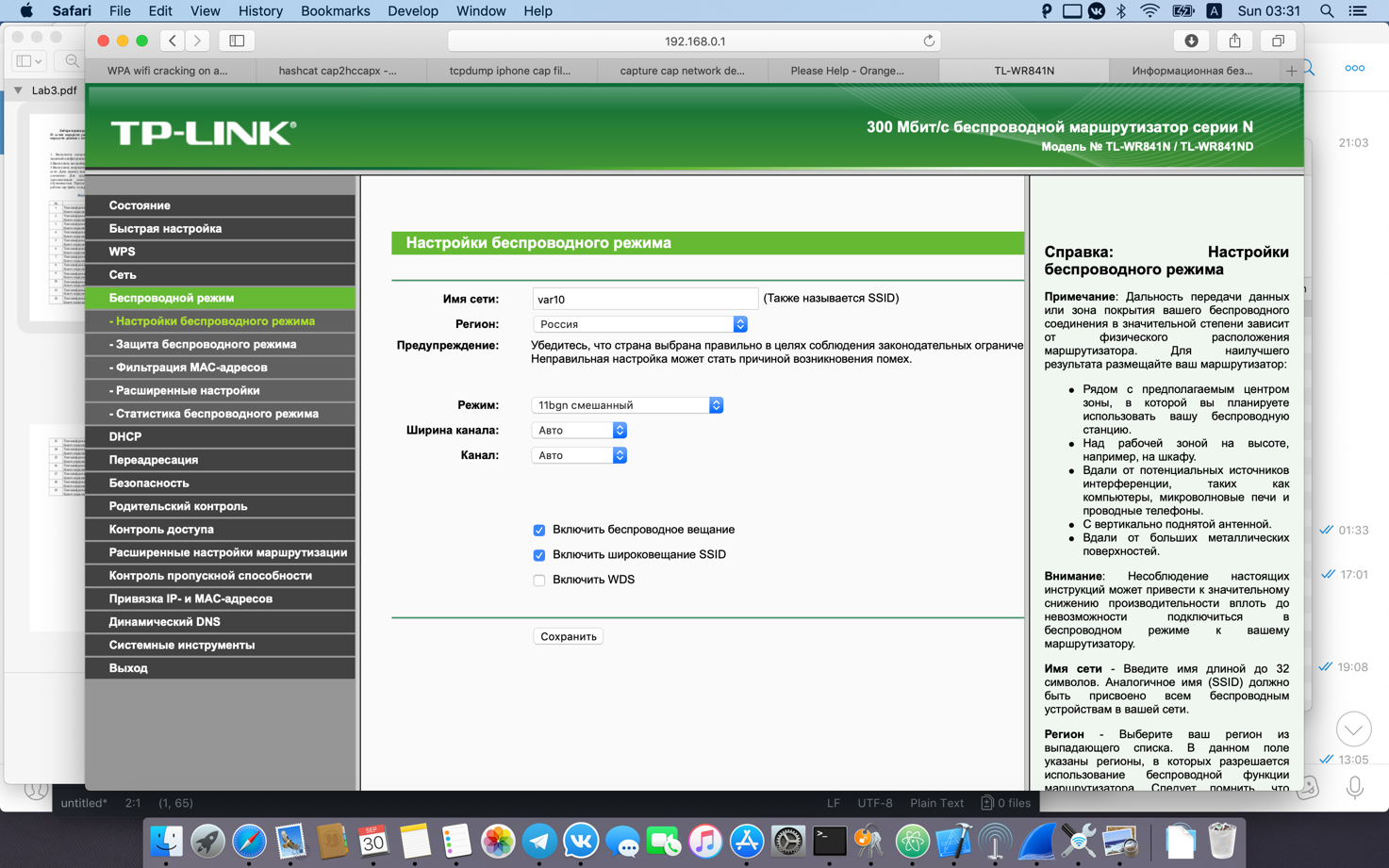


Рисунок 1 – Настройка SSID беспроводной сети

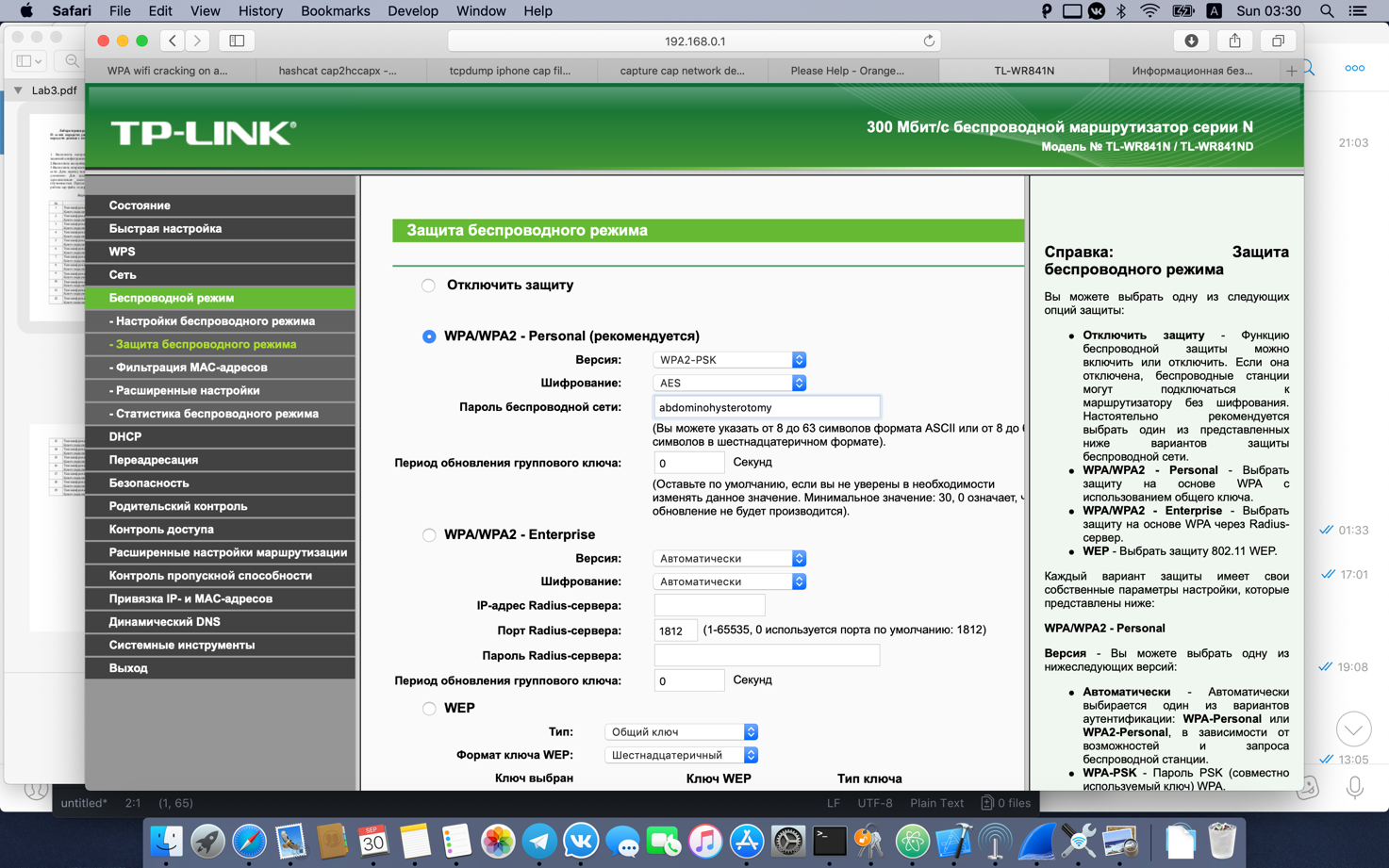


Рисунок 2 – Настройка защиты беспроводной сети

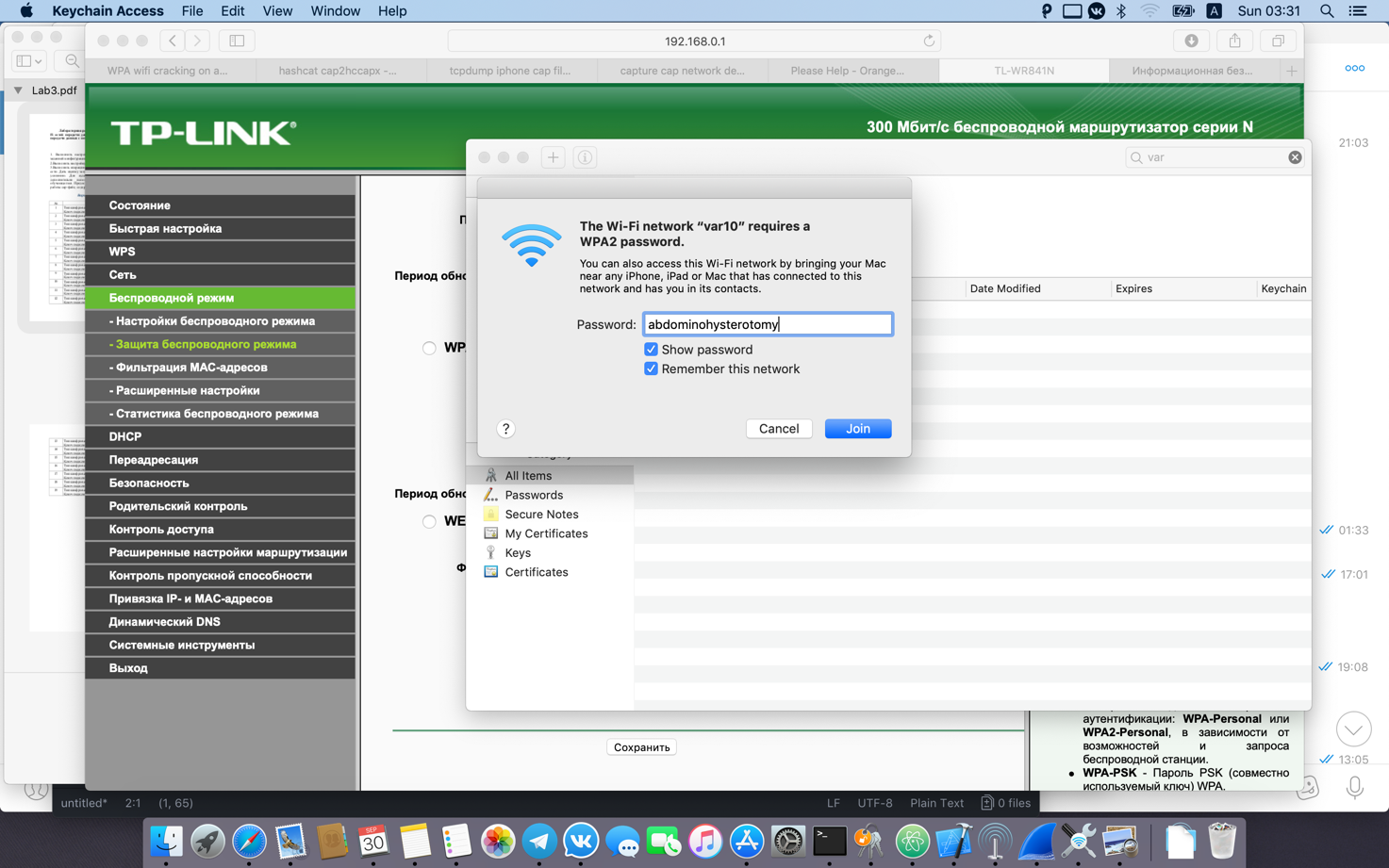


Рисунок 3 – Операция подключения с ОС MacOS X

Ввиду технической невозможно лабораторная работа выполняется на ОС MacOS X. Так как при установке Kali Linux на компьютеры Apple нового поколения отсутствует поддержка драйверов для карт Wi-Fi, чтобы их было возможно перевести в режим прослушивания устройств. Однако есть аналоги данных утилит для MacOS X. С их помощью и выполняется данная работа

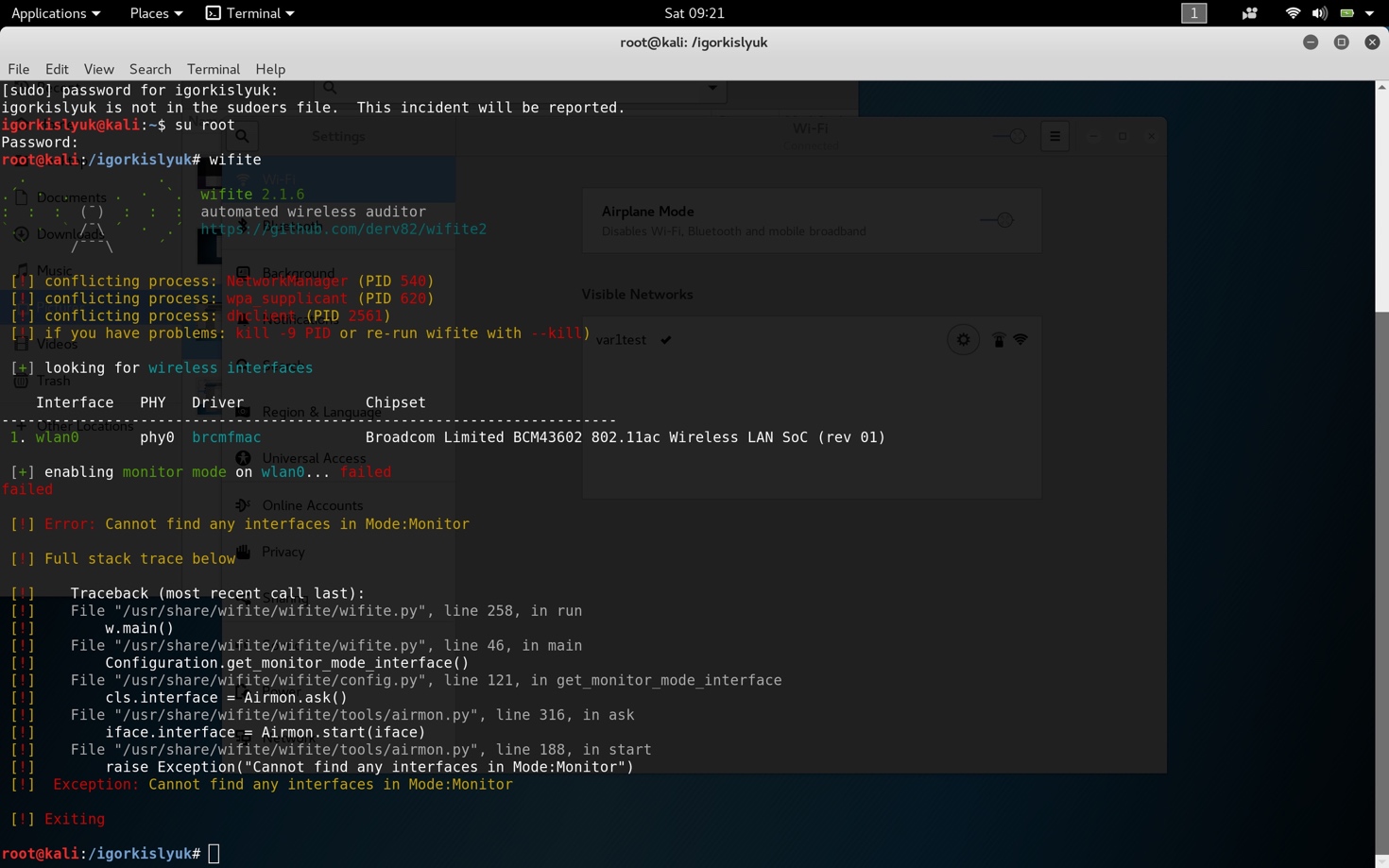


Рисунок 4 – Пример неудачной попытки запустить monitor mode на MacBook c установленным Kali Linux

Утилита Jam Wi-Fi позволяет прослушать входящие соединения.

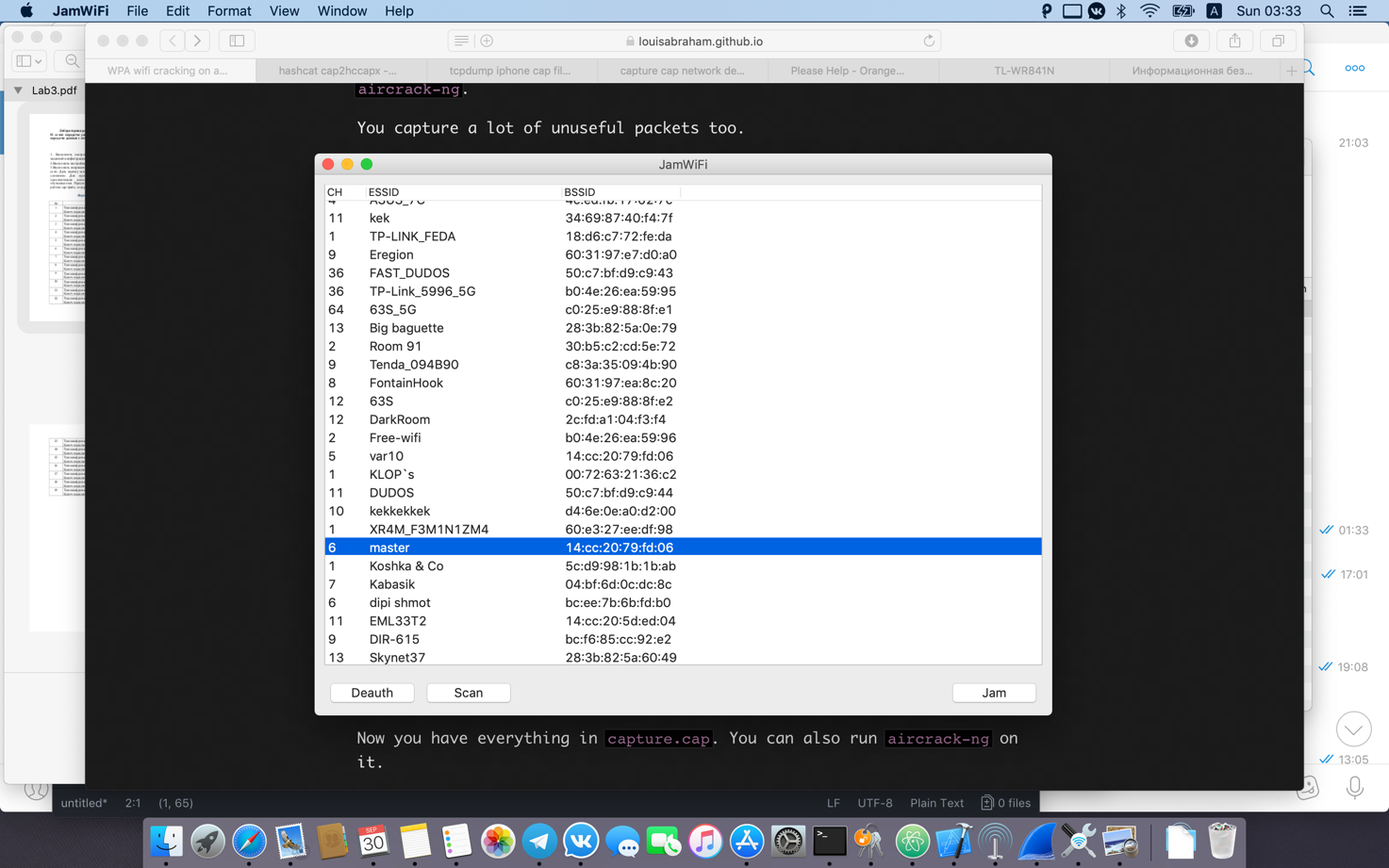


Рисунок 5 – Пример прослушивания существующих сетей

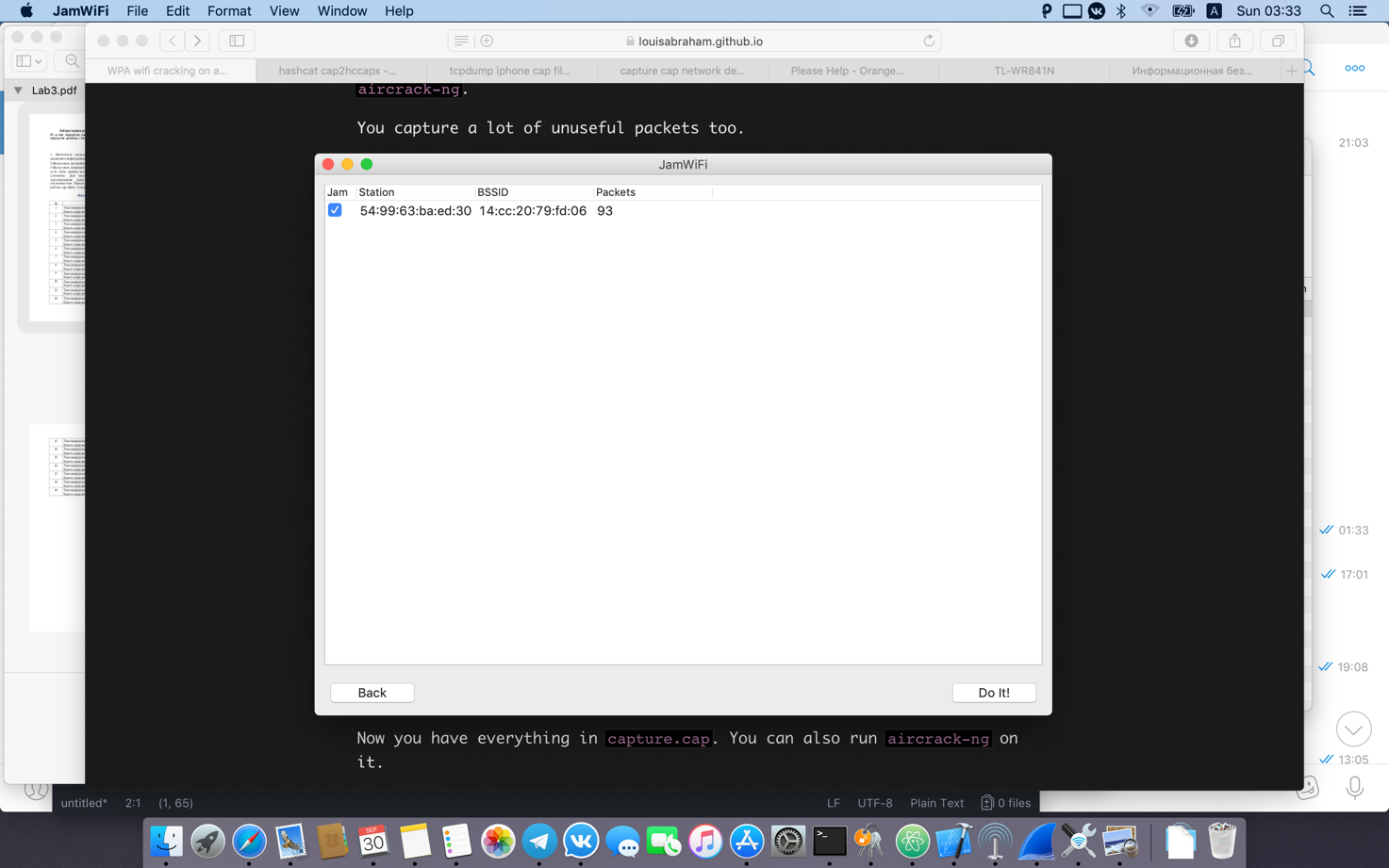


Рисунок 6 – Пример выбора и идентификации целевого устройства

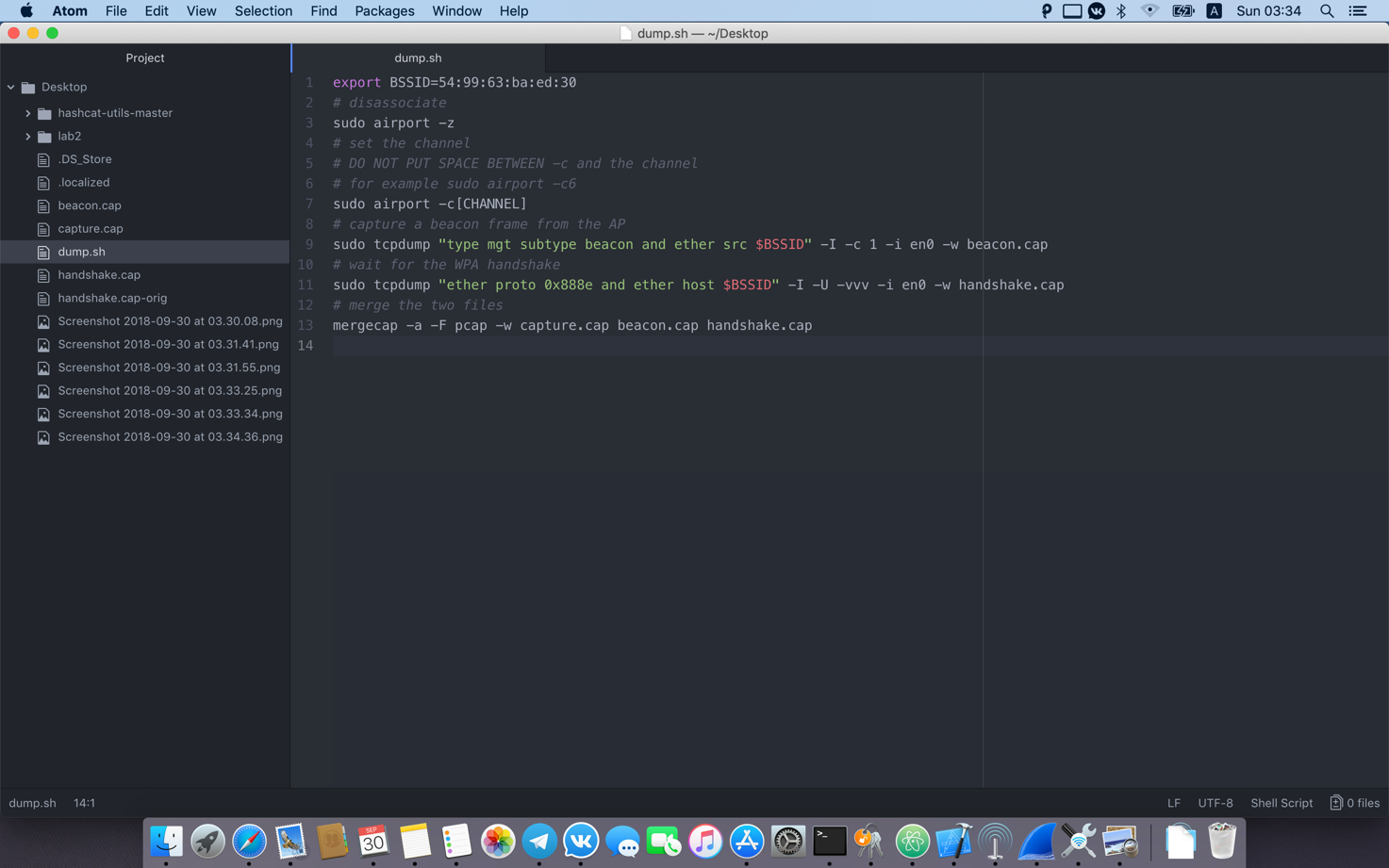


Рисунок 7 – Пример скриптового файла для перехвата необходимых сведений

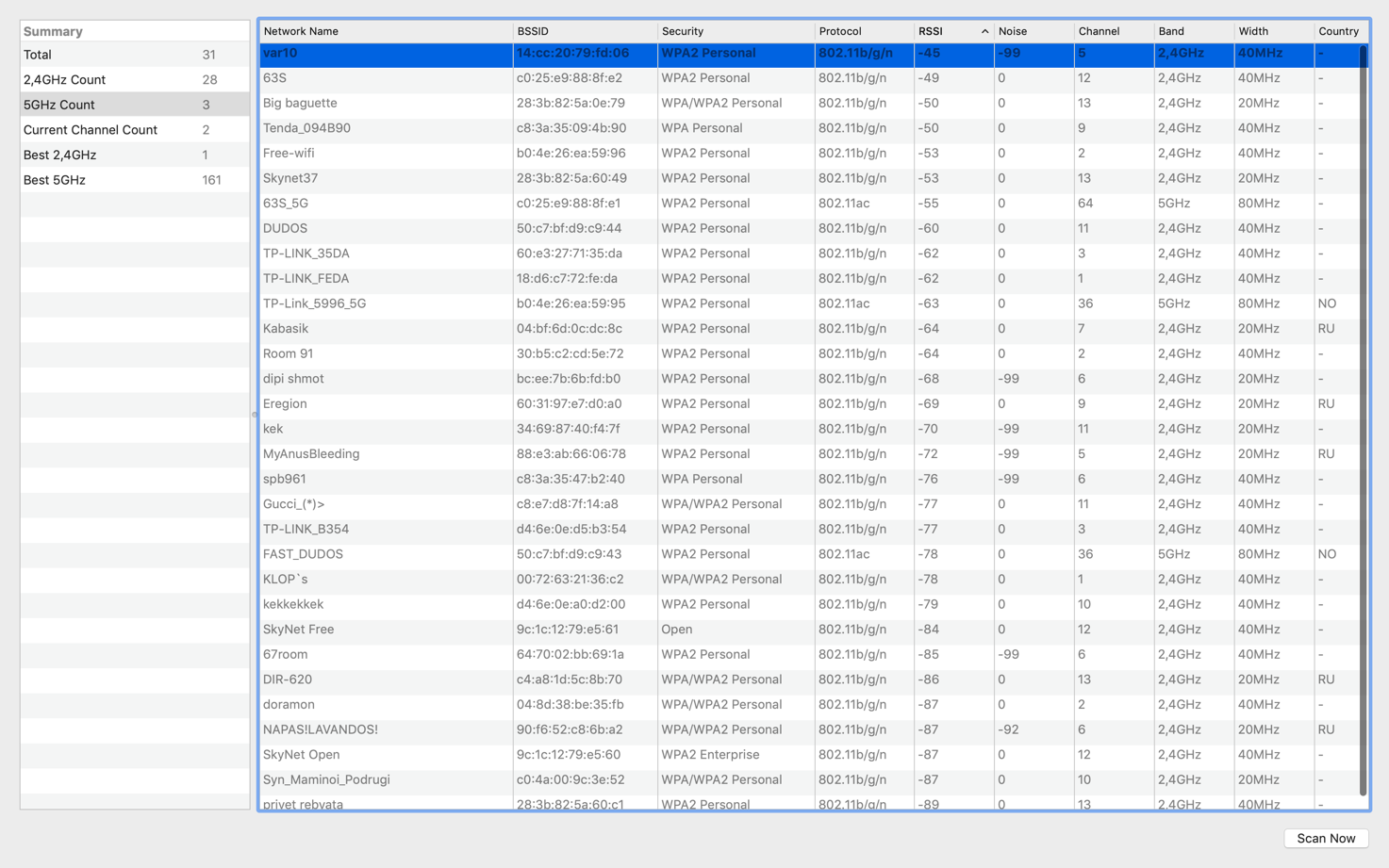


Рисунок 8 – Пример определения BSSID

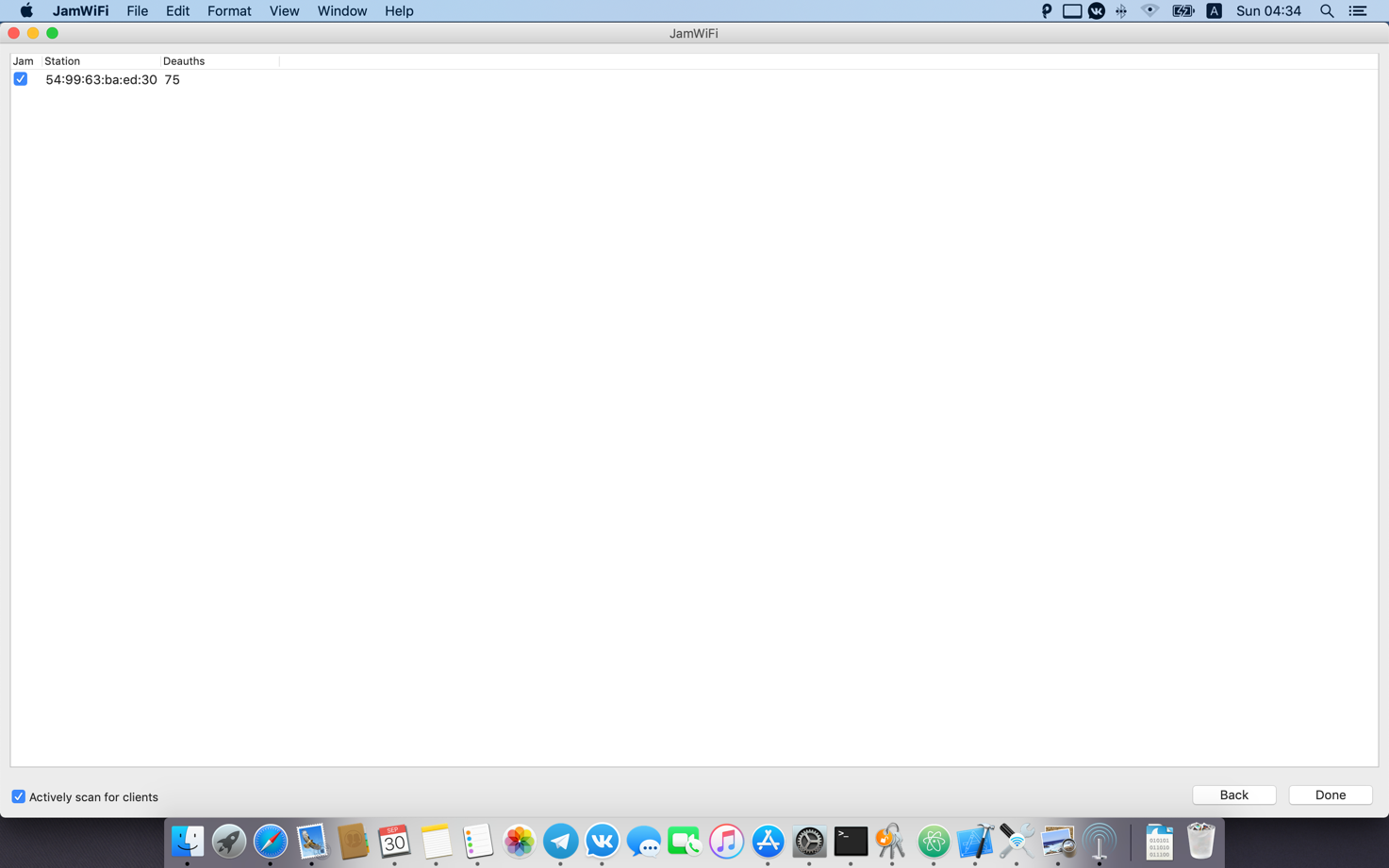


Рисунок 9 – Пример запуска пакетов деавторизации

После успешной деавторизации клиента можно получить необходимые сведения, чтобы расшифровать данные. Все необходимые файлы предоставлены.

## Вывод

В ходе выполнения лабораторной работы были получены знания по работе с перехватом трафика на ОС MacOS X, поскольку для предоставляемых компанией Apple картах беспроводной сети не существует поддерживаемых драйверов на свободно распространяемых ОС. Однако, при необходимости, возможно найти средства взлома и прослушивания трафика для нужной вам системы