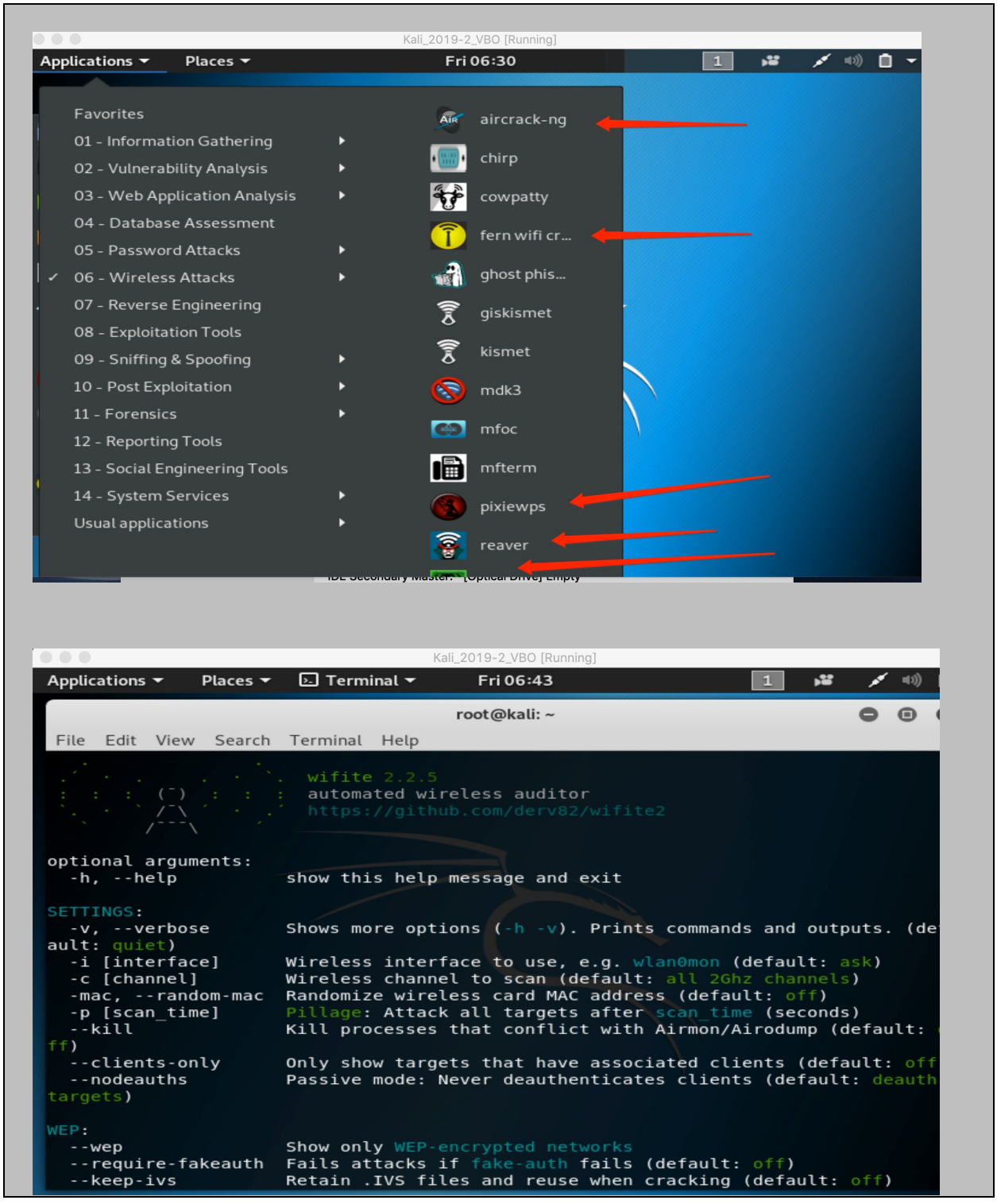
Задание выполнил студент группы 2345 Романенко Кирилл

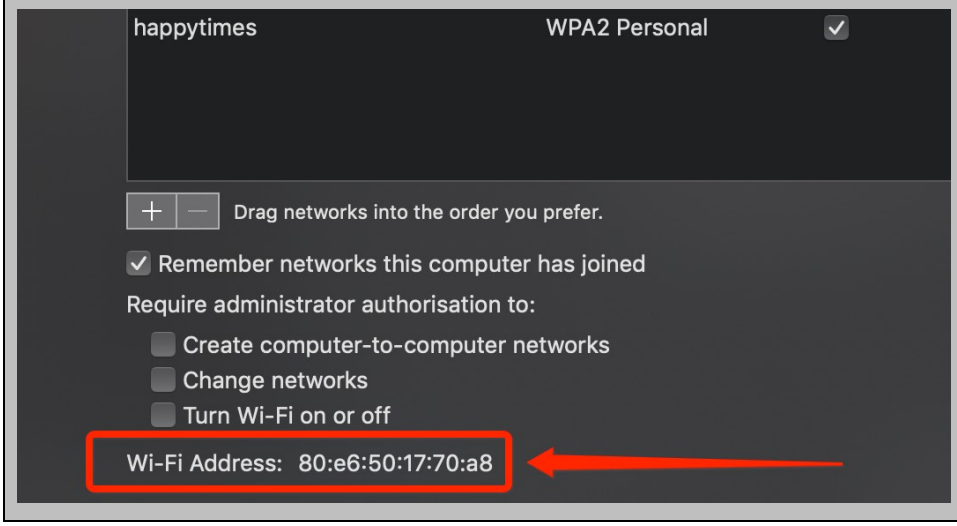
1. Изучить утилиты для работы с Wi-Fi.

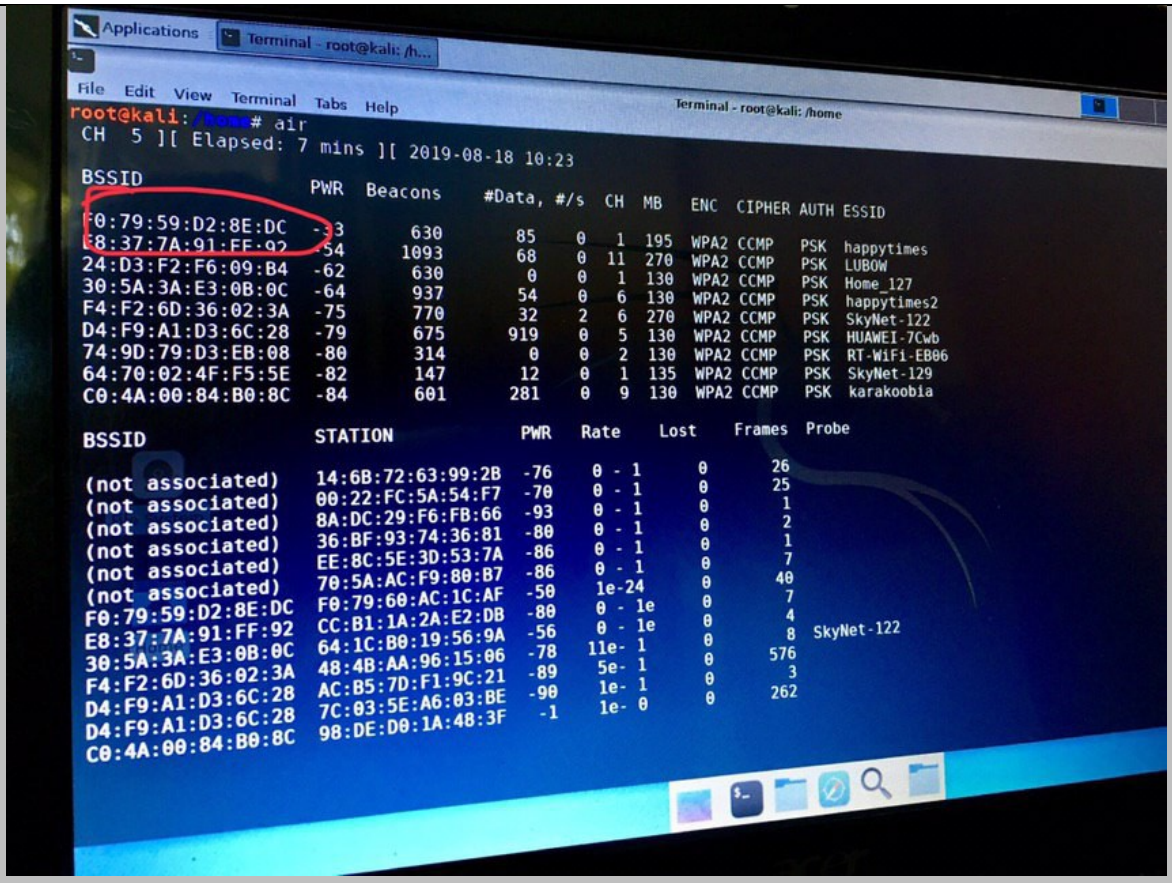


2. Снять дамп соединения утилитой Airodump-ng. Для этого создайте и подключитесь к своей тестовой незащищенной сети. Ввести логин и пароль на несколько сайтов. Найти сайт с незащищенным соединением (http), войти в аккаунт. Найти в дампе cookies от незащищенного сайта.

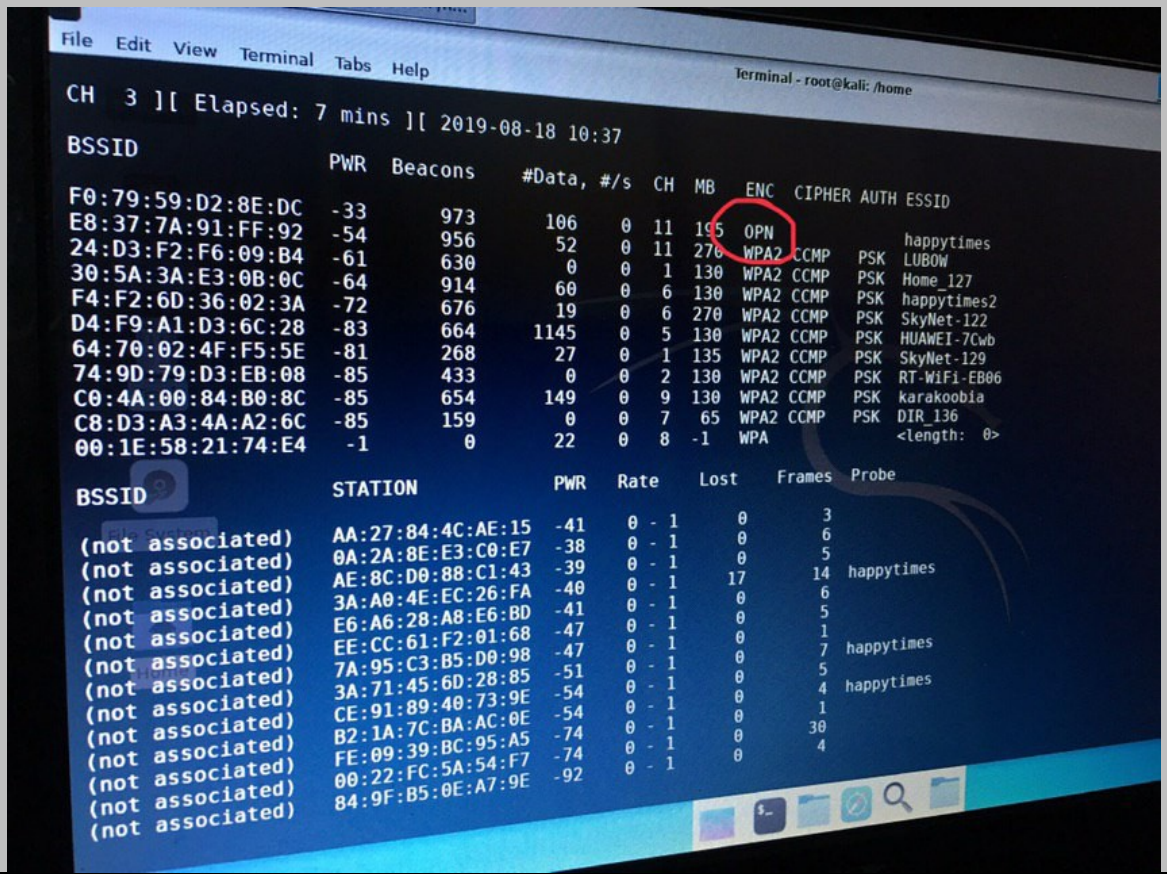
К сожалению на данный момент alfa awus 051nh недоступна - поэтому достаем из кладовки старый добрый asus, запускаем с флешки КАЛИ и переводим адаптер в режим мониторинга, сохраняем все в дамп.

Фиксируем мак адрес точки доступа и вайфай-адаптера мака:

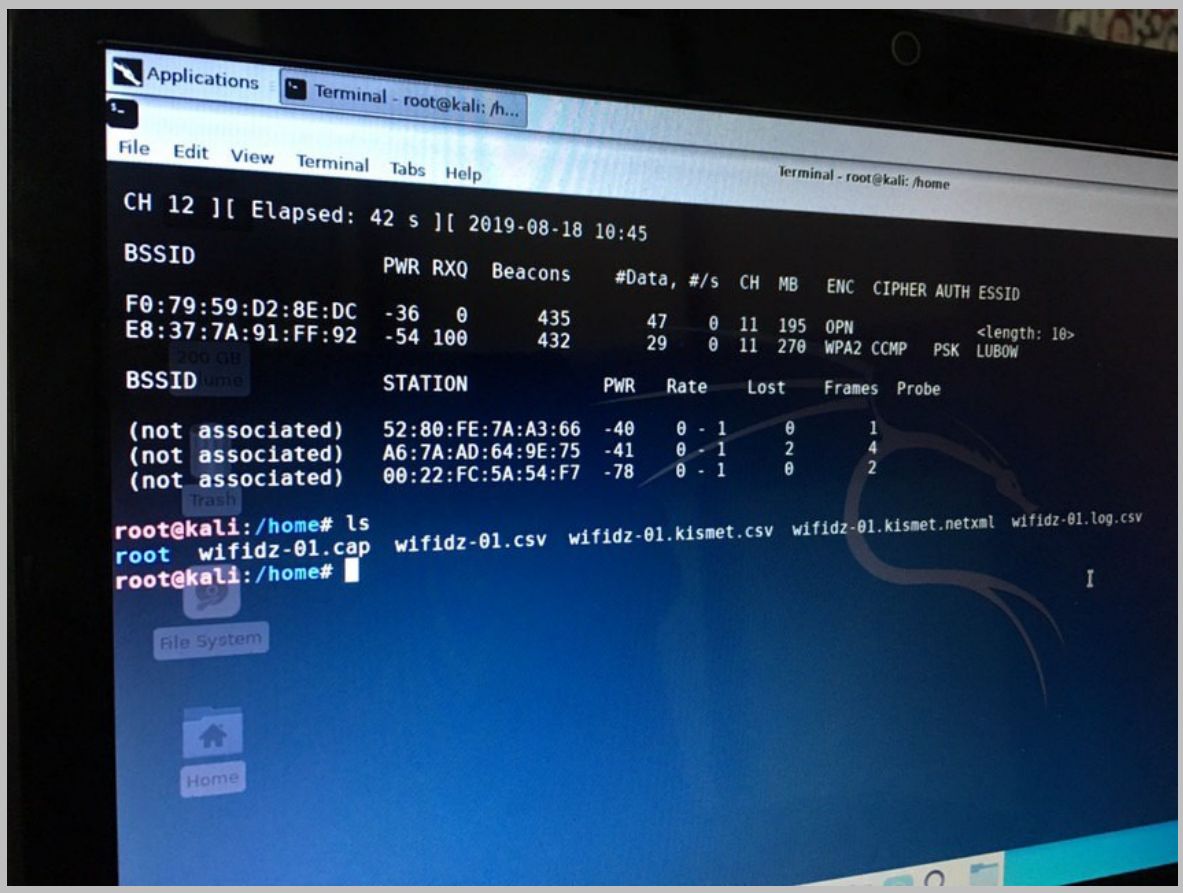


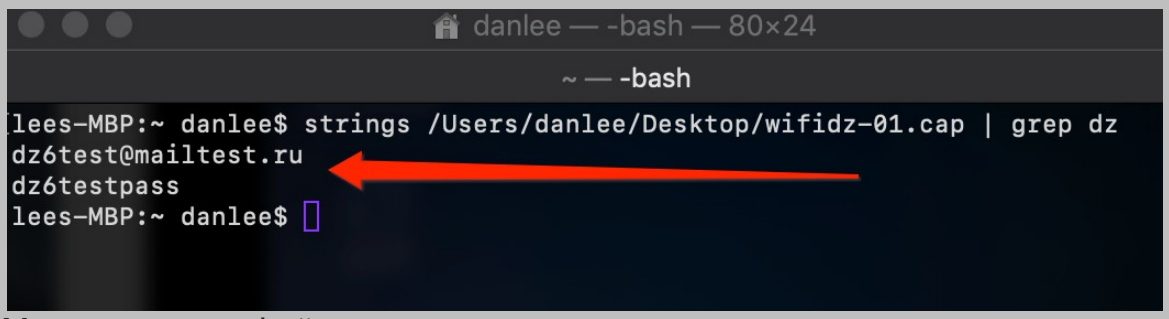


В режиме мониторинга atheros прекрасно ловит в бетонной коробке. Видно много всего и на первом месте нашу тестовую точку (скрытая) - видим на точке PSK.



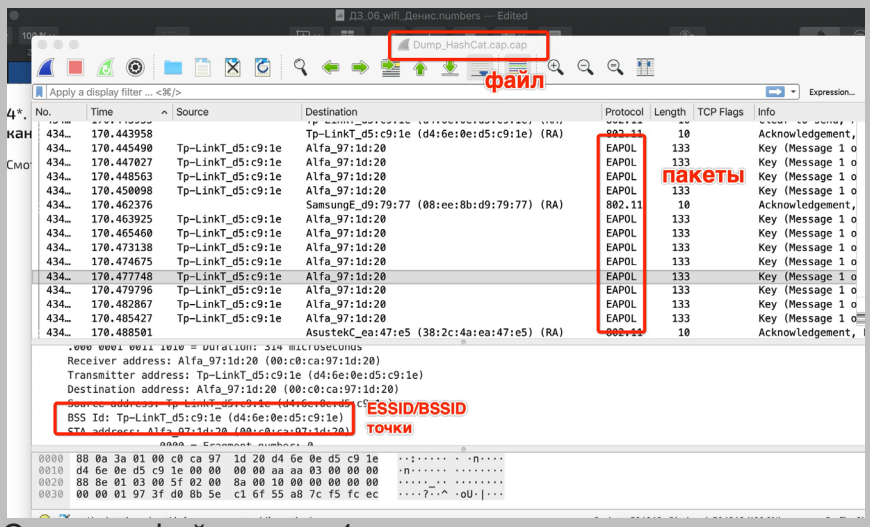
Отключаем шифрование и захватим трафик идущий с нашего тестового компа, зайдем на сайт с авторизацией и без https.





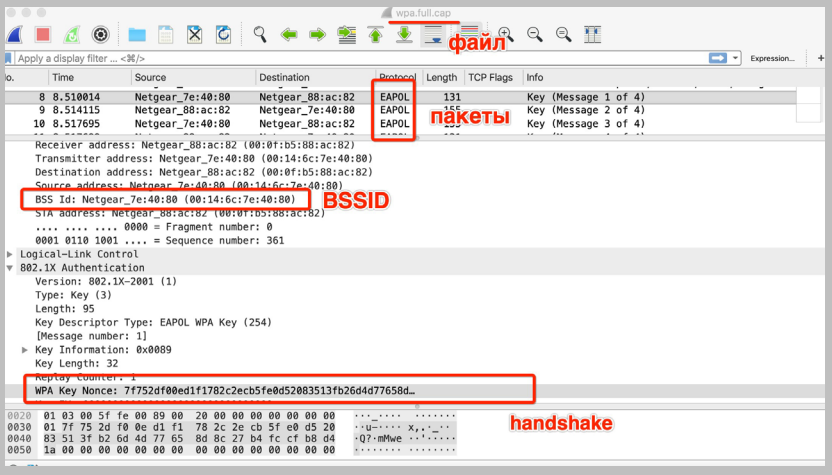
Можно открыть файл в ваершарке, но мы знаем, что искать и поэтому просто найдем в файле наши данные

3. Найти хендшейк в предложенных дампах. Назвать ESSID, BSSID и канал атакованной сети, имя файла с EAPOL-пакетами



Смотрим файл номер 1:

Второй файл, отметим и хэндшейк (вероятно, мост между двумя точками поднимали):



Третий файл из двух частей, где много пакетов с деаутентификацией и как итог пойманные хэндшейки:

Останется время