**Письмо-задание**

Добрый день, уважаемые коллеги!

Вчера поступило сообщение об ограблении банкоматов банка «Надежный» в городе Калининград. Цели расположены по адресам: улица Александра Невского, 193А, улица Кирова, 28 (Лицей № 49) и улица Октябрьская, 68-74. По предварительной информации, полученной от сотрудников безопасности банка, работала группа налетчиков в количестве более трех человек.

Прошу оказать содействие в расследовании инцидента и выявить группу злоумышленников.

P.S. Напоминаю, что в отчете необходимо указать алгоритм поиска и полностью воспроизвести цепочку событий.

С уважением.

**Рекомендации от ведущего аналитика**

Старшие коллеги (aka 5 курс) решают эту задачу без дополнительной информации. Тем не менее, для ускорения процесса рекомендую следующую последовательность действий:

1. Знакомство
   1. Подключиться к серверу БД (веб-интерфейс phpMyAdmin)
   2. Посмотреть, какие данные доступны
2. Привязка геокоординат
   1. Посмотреть активные LAC и CellID, построить таблицу соответствий
   2. Почитать про MCC-MNC коды (<https://ru.wikipedia.org/wiki/MNC>)
   3. Получить координаты базовых станций по известным LAC и CellID, отметить их на Google Maps метками. Для поиска координат можно использовать внешний сервис (раньше работал <https://cellidfinder.com/cells>, сейчас можно попробовать <https://www.opencellid.org> или другой).
   4. По известным в письме адресам выбрать вероятные точки, входящие в маршрут злоумышленников, по точкам выбрать вероятные базовые станции.
3. Поиск последовательно перемещающихся абонентов
   1. Для всех абонентов, которые были на каждой из интересующих точек, выбрать последнее время посещения (можно использовать вспомогательные таблицы)
   2. Из всех абонентов из запроса выше выбрать таких, которые последовательно побывали на всех трёх адресах, т.е. на следующий приходили в более позднее время.
   3. Считать их потенциальными злоумышленниками («подозреваемыми»)
4. Поиск связей
   1. Найти «друзей подозреваемых», т.е. всех, кто звонил и кому звонили «подозреваемые» (список уникальных абонентов)
   2. Найти пересечения списков «друзей подозреваемых» и «подозреваемых»
5. Поиск маршрутов (или водителя-наблюдателя)
   1. Поискать таких абонентов, которые были на тех же точках с большим допуском на время. Может быть, он связывался по результатам преступления с кем-то.

С уважением, Ведущий Аналитик.

**Руководство пользователя по работе с виртуальной машиной.**

Для начала работы необходимо настроить на VMNet1 сеть 192.168.15.0/24 и запустить ВМ. Логин и пароль для входа в ВМ: root 12345.

У ВМ имеются следующие «интерфейсы»:

1. Phpmyadmin – интерфейс для работы с БД. Доступен по адресу <http://192.168.15.203/phpmyadmin> логин - phpmyadmin, пароль – 12345.
2. Установленный пакет OpenSSL. Загружать и доставать файлы из ВМ можно с помощью программы WinSCP.

Подсказка: если не получается подключиться, используйте Wireshark. Также проверьте маршруты, в т.ч. отключенный VPN (иначе возможна ситуация, в будет указан неверный сетевой маршрут).

Работать нужно будет с базой данных «billing», которая содержит три таблицы: billing\_type, main\_billing и persons.

Описание таблиц:

1. **billing\_type –** содержиттипы соединений между абонентами. Поля: id – уникальный идентификатор, billing\_type – тип сеанса связи.
2. **Persons –** содержит информацию об абонентах, их ПДн.

Поля:

* 1. `id` тип int unsigned NOT NULL - уникальный номер абонента',
  2. `soc\_st` - содержит системные данные,
  3. `surname` тип varchar(100) NOT NULL - фамилия, выбрана из списка наиболее часто встречающихся',
  4. `name` тип varchar(100) NOT NULL,
  5. `patronymic` тип varchar(100) NOT NULL,
  6. `move\_template` - содержит системные данные,
  7. `mobile\_operator` тип tinyint(3) unsigned NOT NULL - номер оператора, 1 - МТС, 2 - Мегафон, 3 - Билайн, 4 - Теле-2; ',
  8. `lac\_id` тип int(10) unsigned NOT NULL - начальные координаты LAC (код района ); ',
  9. `cell\_id` тип int(10) unsigned NOT NULL - начальные координаты CellID (код конкретной базовой станции); ',
  10. `imsi` тип bigint(20) unsigned NOT NULL - IMSI, уникальный номер SIM-карты абонента. Уникальный для каждого, первые три цифры "250" - код России, еще две - зависят от оператора);',
  11. `imei` тип bigint(20) unsigned NOT NULL - IMEI, уникальный номер телефона абонента. ;
  12. `msisdn` тип bigint(20) unsigned NOT NULL - MSISDN, тот номер, который люди используют для звонков.

1. **main\_billing –** собственно сам биллинг.

Поля:

* 1. `id` bigint(20) unsigned NOT NULL – уникальный идентификатор,
  2. `billtime` datetime NOT NULL – дата и время начала сеанса связи,
  3. `call\_duration` int(10) unsigned NOT NULL – длительность сеанса связи,
  4. `billing\_type\_id` tinyint(3) unsigned NOT NULL – тип сеанса связи,
  5. `lac\_id` int(10) unsigned NOT NULL,
  6. `cell\_id` int(10) unsigned NOT NULL,
  7. `phone\_b` bigint(20) unsigned NOT NULL – номер абонента, с которым устанавливался сеанс связи,
  8. `abonent\_id` int(10) unsigned NOT NULL – уникальный идентификатор из таблицы persons абонента, запись о котором сделана в биллинге,
  9. `abonentimei` bigint(20) unsigned NOT NULL- уникальный номер телефона абонента запись о котором сделана в биллинге,
  10. `abonentimsi` bigint(20) unsigned NOT NULL - уникальный номер SIM-карты абонента, запись о котором сделана в биллинге,
  11. `abonentphone` bigint(20) unsigned NOT NULL – номер абонента, запись о котором сделана в биллинге,
  12. `reverseabonentphone` bigint(20) - содержит системные данные;
  13. `reversephoneb` bigint(20) u содержит системные данные.