

ИНГУШСКИЙ case



Отчёт об OSINT-расследовании. Ингушский кейс

Начало расследования

10.03.25 группе расследования поступило обращение с просьбой помочь в поиске автора провокационного видео, содержащего ЦП¹ и насилие над девочкой 5-7 лет. Целью расследования было подтверждение или опровержение фактов насилия, а также сбор достаточной доказательной базы и досье для передачи материалов в правоохранительные органы.

Исходные данные

На момент начала расследования имелись следующие зацепки:

- ID в Telegram: 6579652184
- Фотографии, в том числе с самой девочкой
- Видеофиксация надругательства
- Предположительное место проживания

Сбор и анализ информации

Сбор информации начался с поиска зацепок и стилометрии² в группах Telegram. Это мероприятие привело к следующим зацепкам:

- Архив юзернеймов, логинов
- Возможное имя: Фарис
- Возможные фамилии: Леимоев, Радиев, Мариев
- Возможное ФИО: Б*с**в Фарис С*л**м*н*в**
- Место проживания: с. М*****
- Возраст жертвы: 7 лет

Затем, его старый Telegram-юзернейм @Granatovy_06 был использован как основа для дорков³ в разных поисковых системах.



Дорк Telegram-юзернейма

Посредством дорков была найдена публикация в сообществе Молодежь Кавказа 29.04.2020. В публикации фигурант заявил, что ищет себе невесту, и для связи указал свой действующий номер телефона. Используя HLR-запрос⁴ группа расследования получила информацию о том, что номер телефона на данный момент находится в сети. Также, был найден профиль в Одноклассниках искомого, в котором указано, что он проживает в городе Магас.

1 ЦП — аббревиатура child p***** — контент, содержащий половой акт детей или сексуальное насилие над детьми.

2 Силометрия — анализ текста.

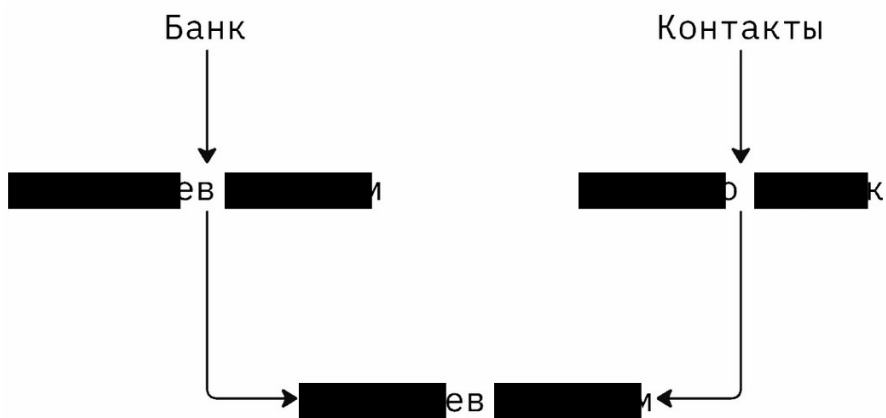
3 Дорк — специфический поисковой запрос с использованием поисковых операторов.

4 HLR-запрос — это технический запрос к центральной базе данных оператора сотовой связи.

+7 (988) 825-18-44 Хочу жену звонить мне | Интересный...
ok.ru › group/56784170516522/topic/156971862405162
@Granatovy_06 если че телеграмм.

Результат дорков

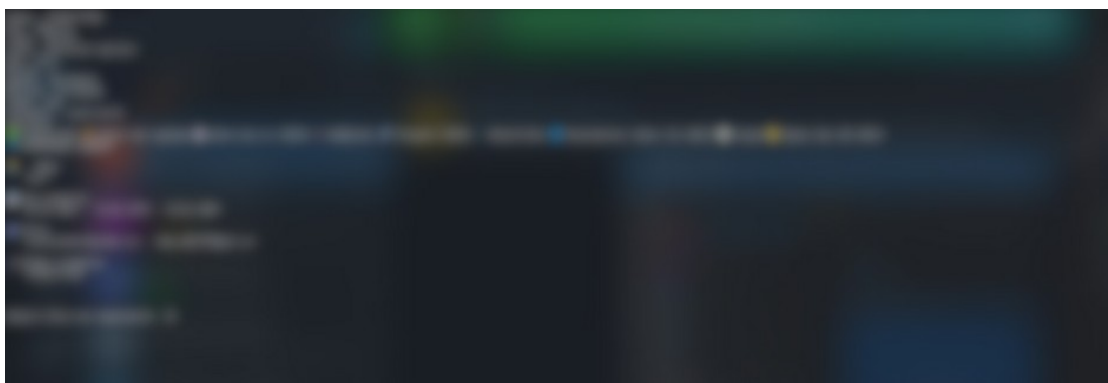
Затем, в контактных книгах были найдены ФИ абонента, использующего номер. Объективность этих данных была подтверждена перекрёстной проверкой через пополнение банковского счёта.



Перекрёстная проверка имени: банк и контактная книга

Однако, из отчета для стилометрии полученные данные не сходятся: фигурант называл себя Фарисом, используя разные фамилии, размывая следы о себе.

Продолжая поиск по Белх***** был найден его профиль в VK. Взяв за основу утечку "VK Parsing 2021", удалось найти привязанный к аккаунту номер телефона, который привёл к его ФИО, актуальному адресу, VIN-номеру машины, паспортным данным и электронной почте.



Сведения из утечек

Из утечек по номеру телефона была найдена вся недостающая информация для составления досье: идентификаторы документов, адрес, ссылки на социальные сети, транспортное средство.

Объективность найденных данных была подтверждена через гос. реестры и инструменты для проверки существования контактных данных, например Ghunt. Сделав запрос в утилиту по электронной почте можно получить выдачу со значением "[+] Stored session loaded.". Это означает, что адрес электронной почты действителен.

```
[+] Stored session loaded !  
[+] Authenticated !
```

Выдача из Ghunt

Заккрытие кейса

Данные об искомом объекте были найдены, собраны, проанализированы, структурированы и переданы в областное ОВД (исходя из места проживания искомого объекта).

Визуализация данных

