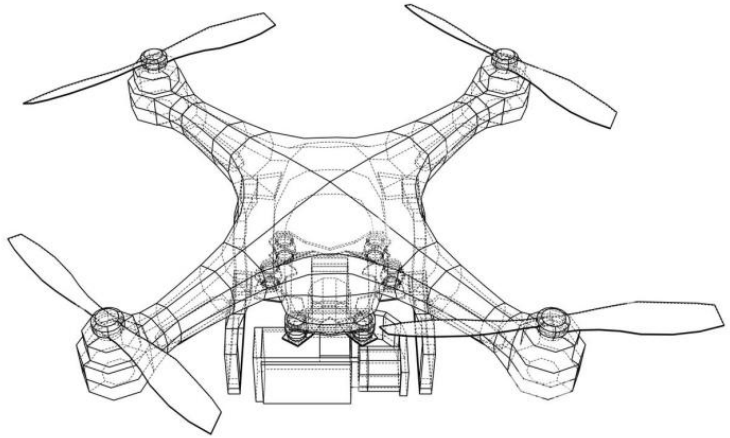

ФОРЕНЗИКА ДРОНОВ

при помощи простых и доступных инструментов

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ФОРЕНЗИКА ДРОНОВ

при помощи простых и доступных инструментов

ИСТОЧНИКИ ПОЛУЧЕНИЯ ИНФОРМАЦИИ

Пульт управления.

Смартфон.

Внешняя память.

Дрон.

БОРОЩУК Дмитрий

BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ. ПУЛЬТ

Пульт управления.

ИЗВЛЕКАЕМЫЕ ДАННЫЕ:

- Серийный номер
- Полетные данные
  - *GPS координаты*
  - *Время по gps*
  - *Скорость/направление/высота*
- Отпечаток сопряженного дрона (Серийный номер)
- Отпечаток сопряженного смартфона (IMEI)
- Параметры радиосигнала

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ. КАНАЛ СВЯЗИ

Дрон.

Пульт управления.

ИЗВЛЕКАЕМЫЕ ДАННЫЕ:

- Отпечаток радио сигнала
- Сигнатура канала связи
- Данные бортового маяка
- Открытый видео поток

АППАРАТНЫЕ ИНСТРУМЕНТЫ:

- HACK RF
- SDR приемник
- WiFi адаптер (monitor mode)
- RTL SDR

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ. КАНАЛ СВЯЗИ

Дрон.

Пульт управления.

ПРОГРАММНЫЕ ИНСТРУМЕНТЫ:

- KISMET

github.com/kismetwireless/kismet
Перехват dji drone id

- DroneScaner

github.com/opendroneid
Приложение для iOS/Android идентификации дронов поддерживающих Open Drone id

- SDR# + модули **RTL1090 и ADSB#**

airspy.com
Универсальный приемник позволяющий принимать сигналы авиа маяков.

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ. СМАРТФОН

Смартфон.

ИЗВЛЕКАЕМЫЕ ДАННЫЕ:

- Личная идентификационная информация
- Полетные данные
  - *GPS*
  - *скорость*
  - *направление/высота*
  - *путь следования*
  - *уровень заряда батареи*
  - *лог управления*
- Записанные фото/видео
- Серийные номера дрона/пульта

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ. СМАРТФОН. ГДЕ ИСКАТЬ

На примере DJI GO

Смартфон.

Путь	Тип данных	Описание
/media/0/DJI/dji.pilot/ LOG/CACHE	Полетные данные	Собраны по количеству активностей
/media/0/DJI/dji.pilot/LOG/CACHE/ NFZ	Полетные данные	Перечень бесполетных зон
/ media/ 0/ DJI/ dji.pilot/ LOG/ERROR_POP_LOG	Полетные данные	Содержит данные когда gps становился недоступным
/ media/ 0 / DJI/ dji. pilot / DJI _RECORD	Медиа	Фото и видео сохраненные в приложение с наименование в формате год_месяц_день_часы_минуты_секунды. Содержат в себе полные метаданные
/ media/0/DJI/ dji.pilot/ Flight Record	Полетные данные, идентификаторы, серийные номера дронов, лог управления	Все данные о полетах собраны по активностям
/media/0/DJI/dji.pilot/CAC HE IMAGE	Медиа	Превью фото и видео

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ

Внешняя память.

Путь	Тип данных	Описание
DJI/dji.pilot/ LOG/CACHE	Полетные данные	Собраны по количеству активностей
DJI/dji.pilot/LOG/CACHE/ NFZ	Полетные данные	Перечень бесполетных зон
DJI/ dji. pilot / DJI _RECORD DCIM	Видео	Видео сохраненные в приложение с наименование в формате год_месяц_день_часы_минуты_секунды. Содержат в себе полные метаданные
DCIM	Фото	FLYXXX
DJI/ dji.pilot/ Flight Record	Полетные данные, идентификаторы, серийные номера дронов, лог управления	Все данные о полетах собраны по активностям вида FLYXXX.dat в дополнение PHARM.log USER.log
DJI/dji.pilot/CAC HE IMAGE	Медиа	Превью фото и видео

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ТИПОЛОГИЯ ДАННЫХ

Дрон.

ИЗВЛЕКАЕМЫЕ ДАННЫЕ:

- Серийный номер
- Отпечаток сопряженного контроллера (Серийный номер)
- Полетные логи (на внешнюю или встроенную память)
- Записанные фото видео (на внешнюю или встроенную память)

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ЧЕМ ИЗВЛЕКАТЬ.

ПОЛЕТНЫЕ ДАННЫЕ:

- CsvView / Datfile

datfile.net

DatCon — это инструмент с открытым исходным кодом, способный анализировать и преобразовывать файлы DJI .dat в различные форматы.например .kml, .csv. Он также имеет возможность вырезать определенные данные в отдельный файл журнала, напримержурналы конфигурации и событий.
CsvView — это аналогичный инструмент от того же разработчика, который можно использовать для анализа данных журнала. Несмотря на имя, оно не ограничивается файлами CSV и может принимать оригинальные журналы .dat. Хотя оба инструмента похожи у них разные возможности и особенности.

- DJI Assistant 2

Dji.com

Родное приложение для дронов dji позволяющее извлекать информацию из полетных логов

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

ЧЕМ ИЗВЛЕКАТЬ.

МЕДИА:

- VLC

Videolan.org

Универсальный медиа проигрыватель

- Metadata++

Metadatapluplus.com

Каталогизатор медиа файлов с мощным инструментов метаданных

БОРОЩУК Дмитрий
BEHOLDERISHERE consulting

СПАСИБО ЗА ВНИМАНИЕ!
Вопросы?

T.ME/BEHOLDERISHERE

investigation & forensic TOOLS

T.ME/ForensicTOOLS