

# **Содержание**

<b>19 Законный перехват .....</b>	3
<i>Разбор трафика .....</i>	3
Оборудование .....	3
Раздел .....	3
Логи разбора трафика .....	10



# 19 Законный перехват

## Разбор трафика

### Оборудование

Для настройки корректной работы раздела Разбора трафика необходимо добавить оборудование типа "Сервер разбора Рсар" в [раздел Управления списка оборудования](#).

Конфигурация оборудования для разбора трафика:

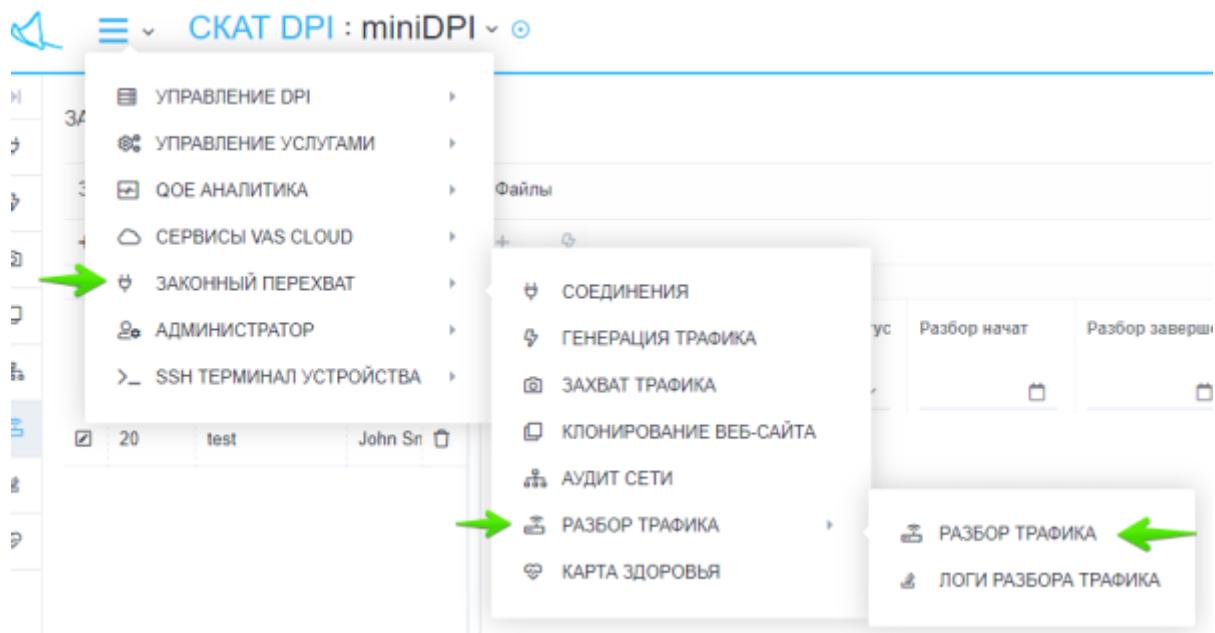
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

Для установки необходимых для работы утилит необходимо выполнить следующую команду:

```
apt install wireshark tshark sox
```

### Раздел

Для перехода в раздел разбора трафика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Разбора трафика".



Раздел Разбора трафика выглядит как на рисунке ниже.

**ЗАКОННЫЙ ПЕРЕХВАТ / РАЗБОР ТРАФИКА**

**Добавить список задач**

**Добавление задачи**

**Добавить файл в задачу**

**Перезапустить разбор трафика для файла**

**Обновить список файлов**

**Редактировать задачу**

**Удалить задачу**

**Редактировать файл**

**Скачать файл**

**Обновить результаты разбора**

**Обновить список**

**Обновить список файлов**

**Обновить список результатов разбора**

**Результаты**

**Web (49)** **Dns (55)** **Mail (1)** **Voice (0)** **Pip (35)**

**Декодированные веб-элементы**

**Запросы** **Изображения**

**Размер** **Метод**

Дата	Урл	Размер	Метод
30.10.2020 08:54:00	oscp.digicert.com	472	GET
30.10.2020 08:53:00	cfd.windowupdate.com/madownload/update/1/static/trusted/visualizedcert/cab7d757d0	0	GET
30.10.2020 08:53:00	cfd.windowupdate.com/madownload/update/1/static/trusted/visualizedcert/cab7d757d1	0	GET
30.10.2020 08:52:00	oscp.digicert.com/	279	GET
30.10.2020 08:51:00	on.kremlin.ru/vyvertavresident/news	0	GET
30.10.2020 08:51:00	on.kremlin.ru/vyvertavresident/newsdata.xml	280	GET
30.10.2020 08:51:00	on.kremlin.ru/static/logo/video.svg	347	GET
30.10.2020 08:51:00	on.kremlin.ru/static/logo/video_text.svg	210	GET
30.10.2020 08:51:00	on.kremlin.ru/static/logo/mail_text.svg	225	GET
30.10.2020 08:51:00	on.kremlin.ru/static/logo/medium_dot.svg	224	GET
30.10.2020 08:51:00	on.kremlin.ru/vyvertavresident/news/calendar/2020	231	GET
30.10.2020 08:51:00	on.kremlin.ru/structure/president/standart	0	GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/Ty6SsBlaAjRATS3O9Rk5t0fERUkA	368035	GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/2GpT384rWYdg	55126	GET

## Задачи

Задачи для Разбора трафика находятся в левой части страницы Разбора трафика.

### Создание задачи

Для создания новой задачи Разбора трафика нажмите на кнопку "+" в туллбаре над списком существующих задач.

**ЗАКОННЫЙ ПЕРЕХВАТ / РАЗБОР ТРАФИКА**

**Добавить задачу**

**Форма создания задачи**

**Разбор трафика**

**Название**

**Описание**

**Отменить** **Сохранить**

В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

### Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.

ID	Задача	Пользователь	Статус
1030_1	Завершена		
0046_1	Завершена		
r-IEEE	Завершена		
р	Завершена		
3624_1	Завершена		
4024_1	Завершена		
рсар	Завершена		

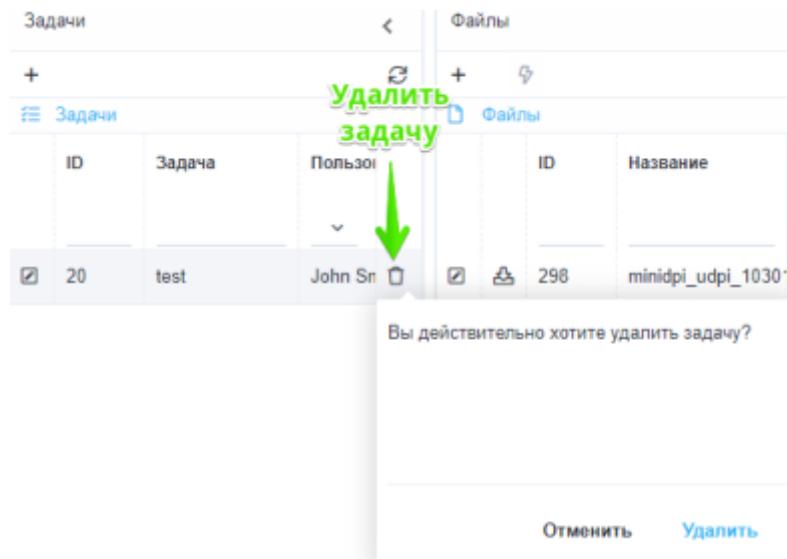
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

### Удаление задачи

Для удаления задачи нажмите на кнопку "Удалить" напротив существующей задачи и подтвердите либо отмените действие.

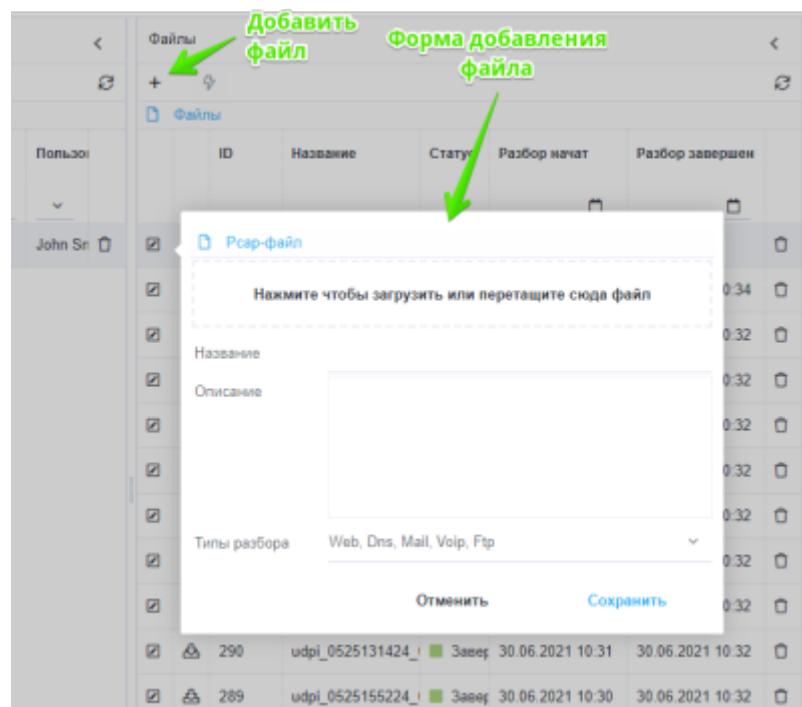


## Файлы

Файлы для Разбора трафика находятся в центральной части страницы Разбора трафика.

### Добавление файла

Для добавления нового файла для Разбора трафика нажмите на кнопку "+" в туллбаре над списком добавленных файлов.



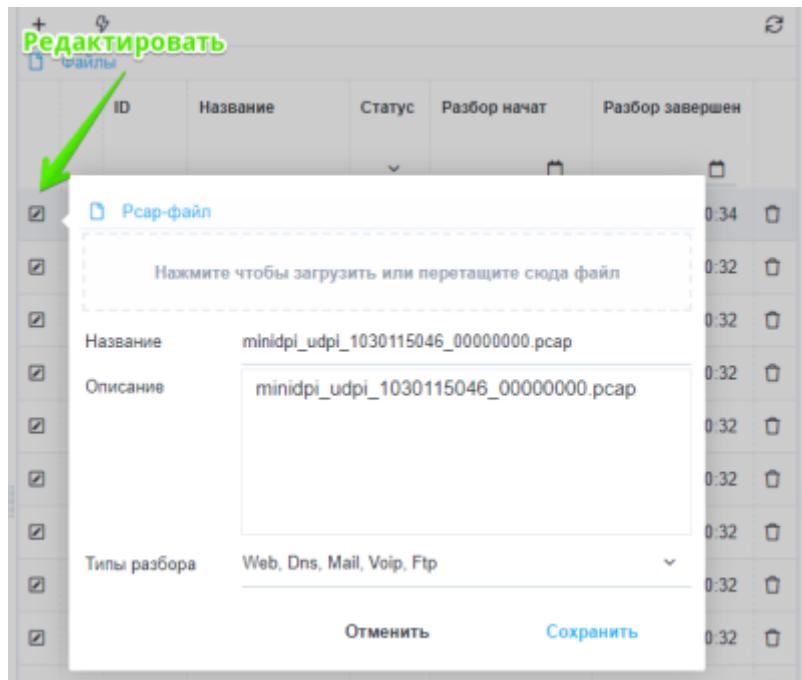
В открывшейся форме добавления файла:

- Загрузите или перетащите рсар-файл;
- При необходимости задайте отображаемое название и описание для файла;
- Укажите необходимые типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

### Редактирование файла

Для редактирования файла для Разбора трафика нажмите на кнопку редактирования напротив существующего файла.



В открывшейся форме редактирования файла можно изменить:

- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

Нажмите кнопку "Сохранить".

В случае, если были внесены изменения в типы разбора трафика - на экране появится форма подтверждения перезапуска разбора трафика для этого файла.

### Удаление файла

Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	294	udpi_0525155624_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить файл"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	293	udpi_0525124024_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	292	email_fuckup.pcap	<span style="background-color: green; color: white;">Завер</span>	20.08.2021 02:31	20.08.2021 02:31	Вы действительно хотите удалить файл?
<input type="checkbox"/>	<input checked="" type="checkbox"/>	291	udpi_0525155424_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	01.07.2021 10:32	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	290	udpi_0525131424_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	289	udpi_0525155224_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	288	udpi_0525131624_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	

## Перезапуск разбора файла

- Для перезапуска разбора файла:
- Выберите необходимый файл из списка;
  - Нажмите на кнопку перезапуска разбора в тулбаре;
  - Подтвердите либо отмените действие.

**Перезапуск**

Файлы

+ ⌂

Вы уверены, что хотите перезапустить очередь для разбора файла?

		Файл	Старт	Разбор завершен			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	294	udpi_0525155624_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:34	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	293	udpi_0525124024_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	292	email_fuckup.pcap	<span style="background-color: green; color: white;">Завер</span>	20.08.2021 02:31	20.08.2021 02:31	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	296	Apple_IP-over-IEEE	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	295	ipv4frags.pcap	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	294	udpi_0525155624_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	293	udpi_0525124024_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	292	email_fuckup.pcap	<span style="background-color: green; color: white;">Завер</span>	20.08.2021 02:31	20.08.2021 02:31	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	290	udpi_0525131424_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	01.07.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	289	udpi_0525155224_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	288	udpi_0525131624_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	287	udpi_0525131524_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	286	udpi_0525155524_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	285	udpi_0525155324_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	284	udpi_0525124124_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	283	udpi_0525131324_	<span style="background-color: green; color: white;">Завер</span>	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>

Выделенный файл

Отменить Перезапустить

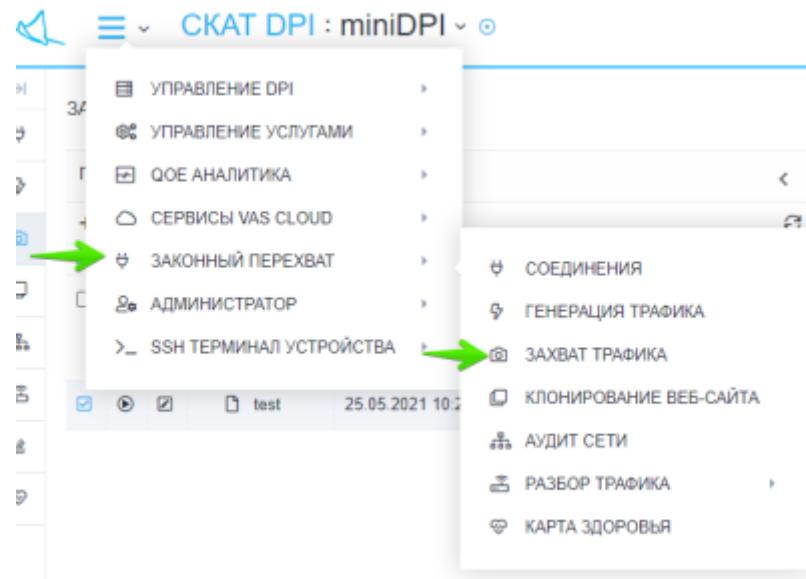
Подтвердить перезапуск

<< < > >> 1 На странице 100

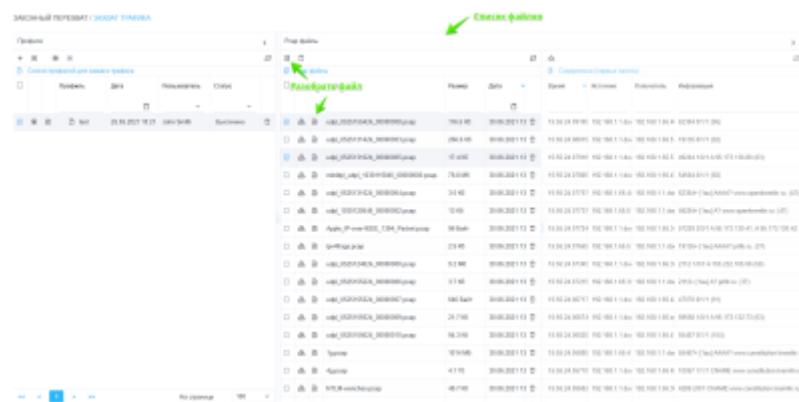
## Импорт файлов из раздела захвата трафика

Файлы для разбора трафика можно импортировать из раздела "Захват трафика".

Перейдите в раздел "Законный перехват"→"Захват трафика".

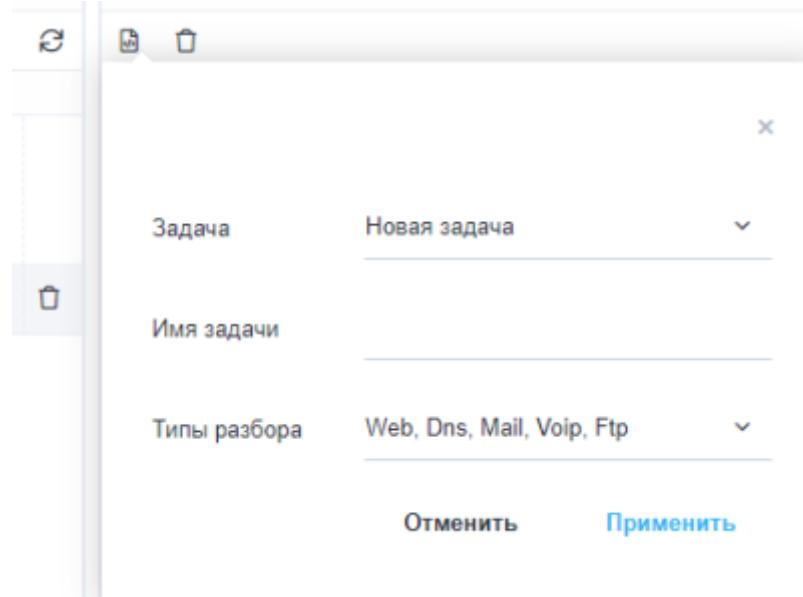


В списке файлов выберите файлы, которые необходимо разобрать и нажмите кнопку разбора.



В открывшейся форме:

- Выберите задачу Разбора трафика, в которую будут импортированы файлы.
- В случае выбора "Новой задачи" - введите имя задачи, которая будет создана при импорте.
- Типы разбора для импортируемых файлов (Web,Dns,Mail,Voip,Ftp).



Нажмите на кнопку "Применить". После завершения процесса импорта файлов появится окно с предложением о переходе в раздел "Разбор трафика".

## Результаты разбора

**Web**

**DNS**

**Mail**

**Voip**

**Ftp**

## Логи разбора трафика

Для перехода в раздел логов разбора трафика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Логи разбора трафика".

СКАТ DPI : miniDPI

- УПРАВЛЕНИЕ DPI
- УПРАВЛЕНИЕ УСЛУГАМИ
- ЮЕ АНАЛИТИКА
- СЕРВИСЫ VAS CLOUD
- ЗАКОННЫЙ ПЕРЕХВАТ**
- АДМИНИСТРАТОР
- SSH ТЕРМИНАЛ УСТРОЙСТВА

291	01.07.2021 10:32:00	Pcap
275	01.07.2021 10:32:00	Pcap
291	01.07.2021 10:32:00	Pcap
275	01.07.2021 10:32:00	Pcap

РАЗБОР ТРАФИКА

- СОЕДИНЕНИЯ
- ГЕНЕРАЦИЯ ТРАФИКА
- ЗАХВАТ ТРАФИКА
- КЛОНИРОВАНИЕ ВЕБ-САЙТА
- АУДИТ СЕТИ
- РАЗБОР ТРАФИКА**
- КАРТА ЗДОРОВЬЯ

Действие

- UpdateFileData
- UpdateFileData
- UpdateFileData
- UpdateFileData

Логи разбора трафика

Раздел Логов разбора трафика выглядит как на рисунке ниже.

СКАТ DPI : miniDPI

ЗАКОННЫЙ ПЕРЕХВАТ / ЛОГИ РАЗБОРА ТРАФИКА

Обновить список задач

Удалить задачу

Просмотр информации о задаче

Постстраничный переход

Количество записей на странице