

Table of Contents

19 Законный перехват	3
Разбор трафика	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:

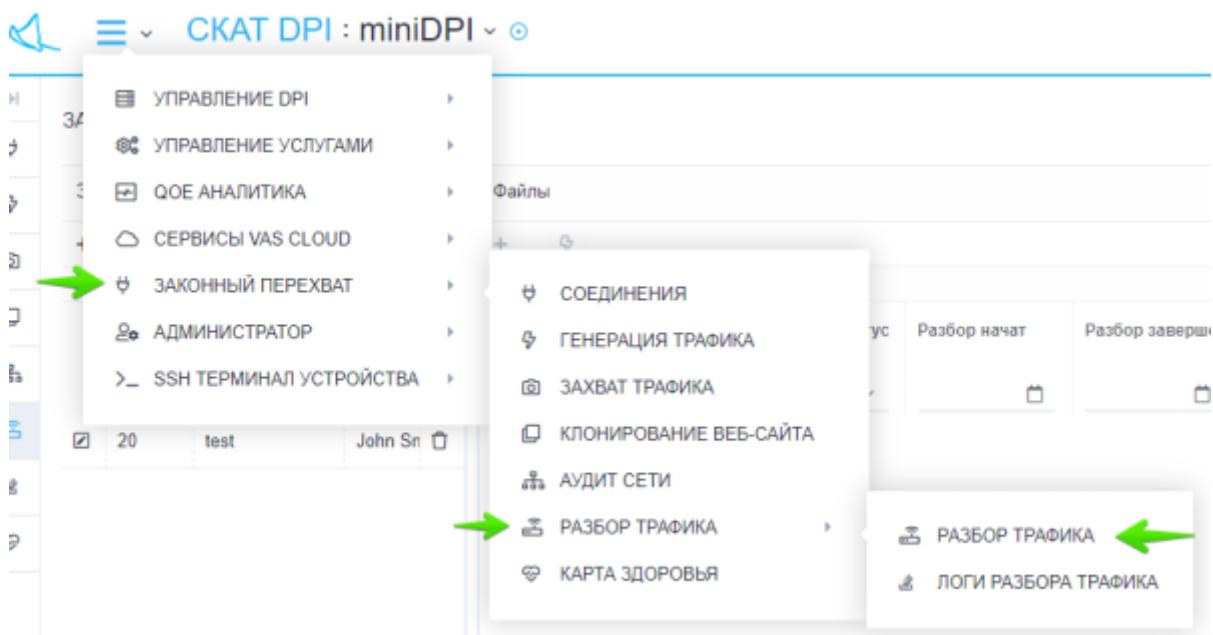
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

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.

Скриншот интерфейса CKAT DPI, демонстрирующий разделы Задачи и Файлы, а также таблицу результатов разбора трафика.

Задачи (Tasks):

- Кнопка **Добавление задачи** (+) для создания новой задачи.
- Кнопка **Добавить файл** для добавления файла в существующую задачу.
- Кнопка **Перезапустить разбор трафика для файла** для перезапуска анализа выбранного файла.
- Кнопка **Удалить задачу** для удаления задачи.
- Кнопка **Редактировать задачу** для редактирования существующей задачи.
- Кнопка **Скачать файл** для загрузки выбранного файла.

Файлы (Files):

- Кнопка **Обновить список файлов** для обновления списка файлов.
- Кнопка **Обновить результаты разбора** для обновления результатов анализа.

Обработка результатов (Processing results):

Результаты	Web (49)	Dns (55)	Mail (1)	Voip (0)	Pip (35)
Декодированные веб-элементы					
Запросы					
Изображения					
Дата	Урл	Размер	Метод		
30.10.2020 08:54:00	oscp.digicert.com/	472	GET		
30.10.2020 08:53:00	cid:windowsupdate.com/madownload/update/1/static/trusted/visual/lovewcert1.cat?14757d0	0	GET		
30.10.2020 08:52:00	oscp.digicert.com/	279	GET		
30.10.2020 08:51:00	on.kremlin.ru/vyvert/tyrident/news	0	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/krasovskihata.wsg	280	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/krasovskihata.wsg	347	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/krasovskihata.wsg	210	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/krasovskihata.wsg	225	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/krasovskihata.wsg	224	GET		
30.10.2020 08:51:00	on.kremlin.ru/vyvert/tyrident/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/Ty6SsBlaAjQRAT309Rk5t0JERUkA	368035	GET		
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/Ty6SsBlaAjQRAT309Rk5t0JERUkA	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.

Скриншот формы создания задачи, отображающей раздел **Разбор трафика**.

Форма создания задачи (Create Task Form):

Кнопка **Добавить задачу** (+) для создания новой задачи.

Разбор трафика (Traffic Analysis):

Поля для ввода **Название** и **Описание**.

Кнопки **Отменить** и **Сохранить** для завершения создания задачи.

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
1030	Задача 1	Пользователь 1
0046	Задача 2	Пользователь 2
91EEE	Задача 3	Пользователь 3
9624	Задача 4	Пользователь 4
4024	Задача 5	Пользователь 5
9999	Задача 6	Пользователь 6

ID	Название	Статус
1030	Задача 1	Завершена
0046	Задача 2	Завершена
91EEE	Задача 3	Завершена
9624	Задача 4	Завершена
4024	Задача 5	Завершена
9999	Задача 6	Завершена

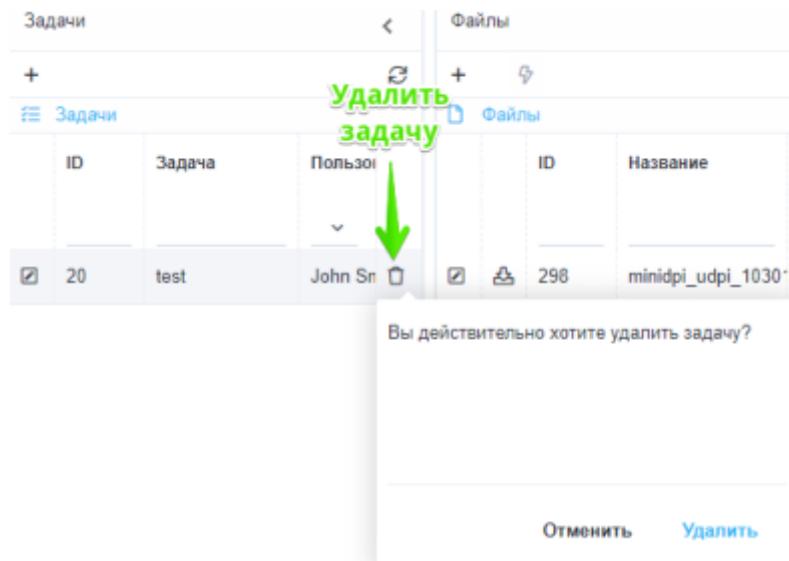
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

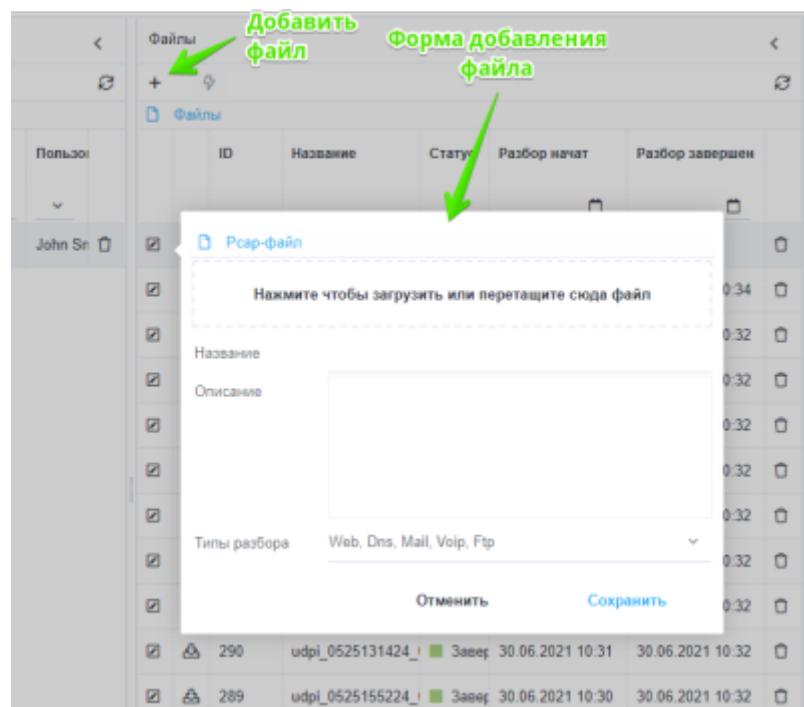


Файлы

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.



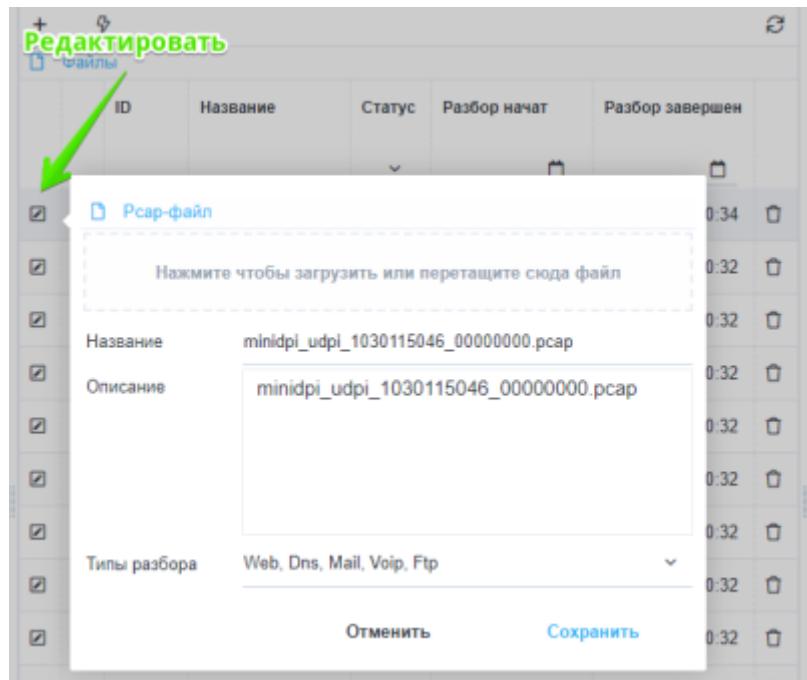
В открывшейся форме добавления файла:

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

Перезапуск разбора файла

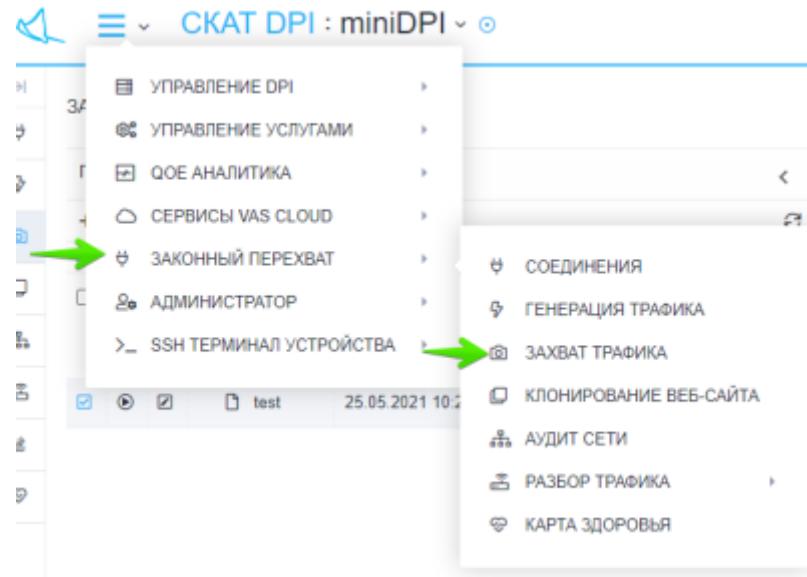
- Для перезапуска разбора файла:
1. Выберите необходимый файл из списка;
 2. Нажмите на кнопку перезапуска разбора в тулбаре;
 3. Подтвердите либо отмените действие.

Перезапуск						
Файлы		Вы уверены, что хотите перезапустить очередь для разбора файла?				
		Файл	Статус	Время начал	Время завершения	
<input checked="" type="checkbox"/>			Завер.	30.06.2021 10:31	30.06.2021 10:34	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>			Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	296	Apple_IP-over-IEEE	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	295	ipv4frags.pcap	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	294	udpi_0525155624_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	293	udpi_0525124024_	Завер.	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	292	email_fuckup.pcap	Завер.	20.08.2021 02:31	20.08.2021 02:31	<input type="button" value="Удалить"/>
Выбранный файл		udpi_0525155424_	Завер.	30.06.2021 10:31	01.07.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>		udpi_0525131424_	Завер.	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	289	udpi_0525155224_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	288	udpi_0525131624_	Завер.	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	287	udpi_0525131524_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	286	udpi_0525155524_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	285	udpi_0525155324_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	284	udpi_0525124124_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>
<input checked="" type="checkbox"/>	283	udpi_0525131324_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value="Удалить"/>

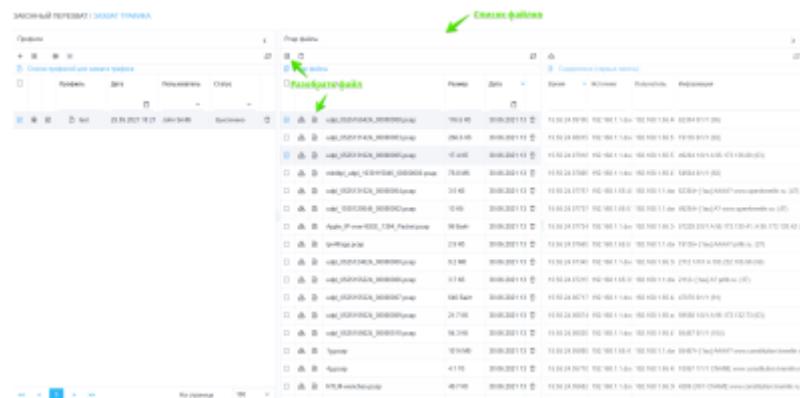
Импорт файлов из раздела захвата трафика

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

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

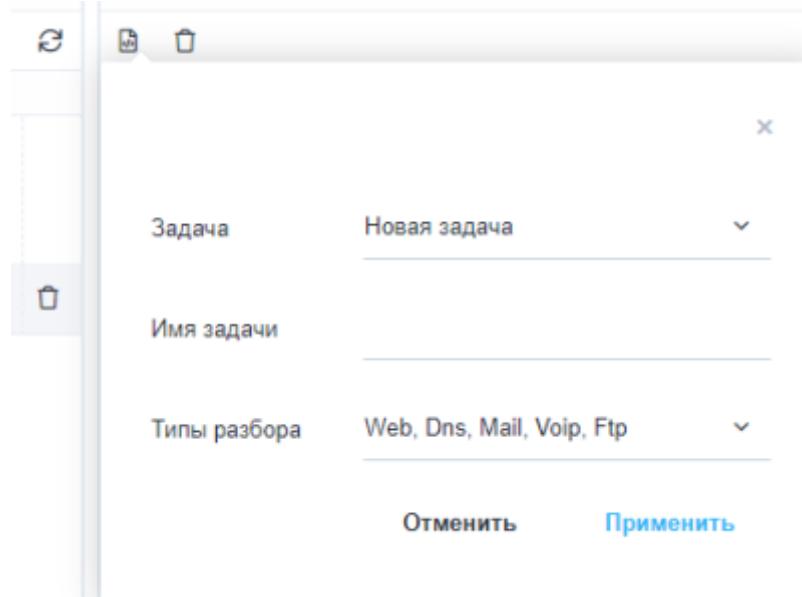


В списке файлов выберите файлы, которые необходимо разобрать и нажмите кнопку разбора.



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".

Раздел Логов разбора трафика выглядит как на рисунке ниже.