

Содержание

19 Законный перехват	3
Разбор трафика	3
Оборудование	3
Раздел	3
Логи разбора трафика	6

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:

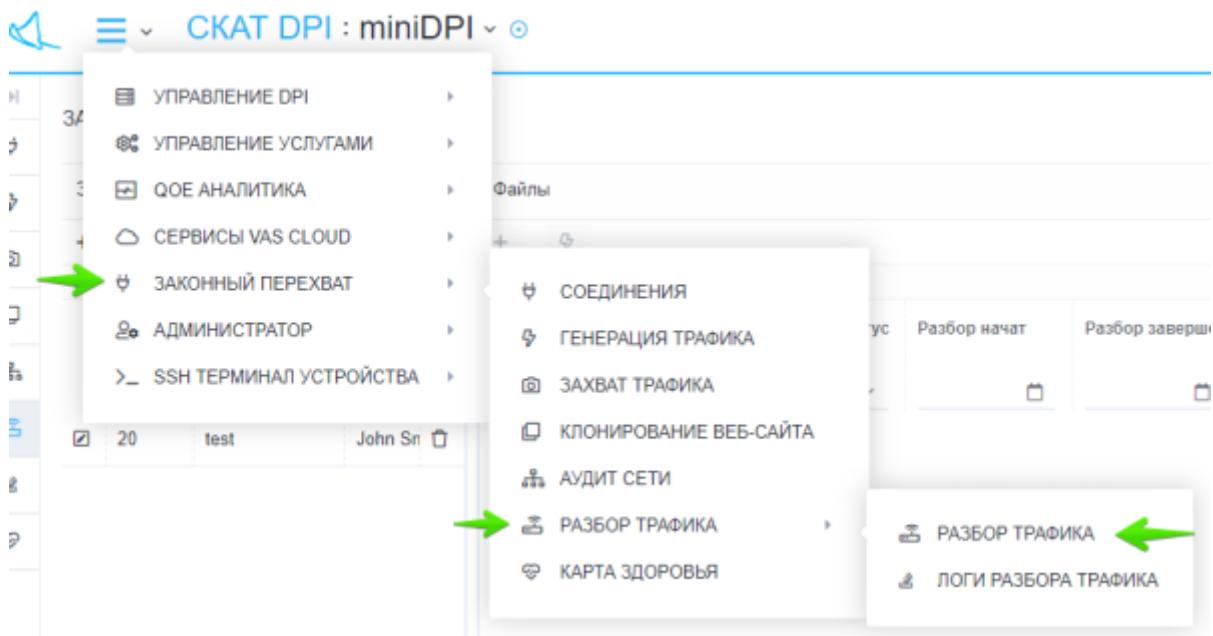
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

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)	Voice (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/visualizedcertcab7d757d0	0	GET		
30.10.2020 08:52:00	oscp.digicert.com/	279	GET		
30.10.2020 08:51:00	on.kremlin.ru/vyvert/voresident/news	0	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/clicks/visualizeddata.svg	280	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/clicks/video.svg	347	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/img/visualized_text.svg	210	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/img/visualized_text.svg	225	GET		
30.10.2020 08:51:00	on.kremlin.ru/static/img/visualized_medium_text.svg	224	GET		
30.10.2020 08:51:00	on.kremlin.ru/vyvert/voresident/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/Ty6SsBlaAjR4TS3O9Rk5t0fERUkA	368035	GET		
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/250T384rWYdg	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 диалогового окна создания задачи, отображающего форму для разбора трафика.

Форма создания задачи (Create Task Form):

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

Разбор трафика (Traffic Analysis):

Поля для ввода **Название** (Name) и **Описание** (Description).

Кнопки **Отменить** (Cancel) и **Сохранить** (Save).

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
1	test	Завершена

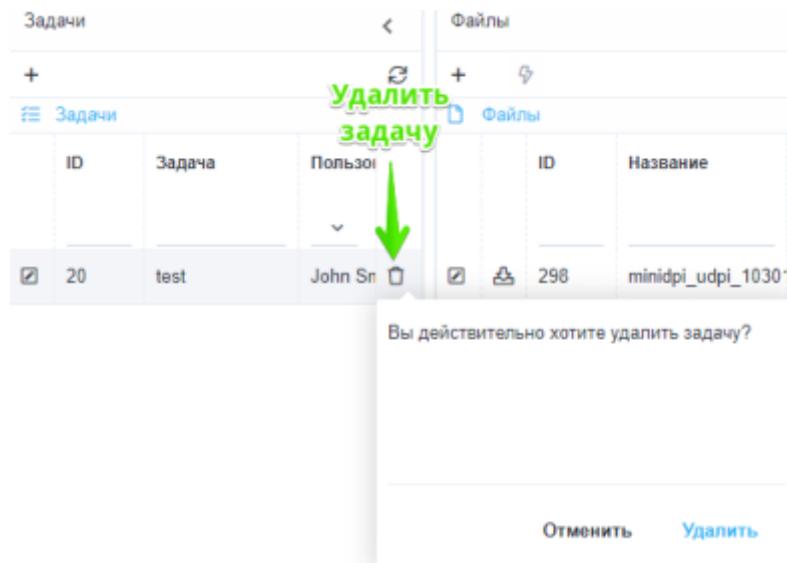
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

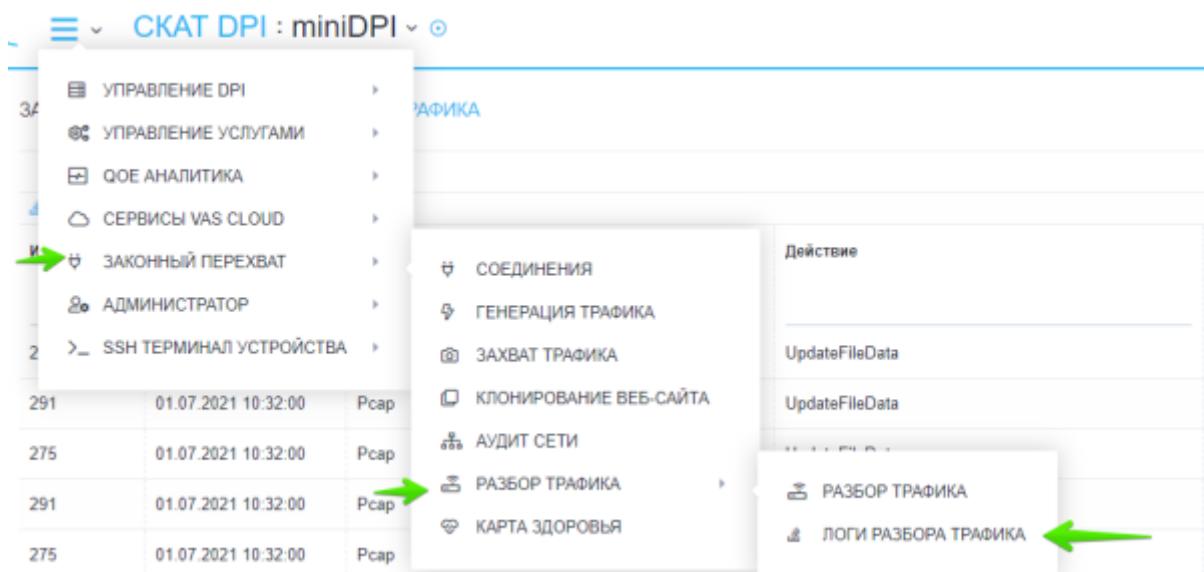


Файлы

Результаты разбора

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.

ЗАМОННІЙ ПЕРЕХВАТ І ПОЛІ РАБОТЫ ТРУДІВКА							Обновить список задач
ID	Суміжні	Дата	Тек	Дії відмін	Теку роботи	Статус	Операції
215	215	01.07.2021 18:32:00	Розр	UpdateFileData	Розр	Ініціюю	 
216	216	01.07.2021 18:32:00	Розр	UpdateFileData	Розр	Ініціюю	 
217	217	01.07.2021 18:32:00	Розр	UpdateFileData	Вір	Ініціюю	 
218	218	01.07.2021 18:32:00	Розр	ParseDecodeData	Розр	Ініціюю	 
219	219	01.07.2021 18:32:00	Розр	UpdateFileData	Мал	Ініціюю	 
220	220	01.07.2021 18:32:00	Розр	UpdateFileData	Онл	Ініціюю	 
221	221	01.07.2021 18:32:00	Розр	UpdateFileData	Web	Ініціюю	 
222	222	01.07.2021 18:31:00	Розр	ParseDecodeData	Розр	Ініціюю	 
223	223	01.07.2021 18:31:00	Розр	ParseDecodeData	Вір	Ініціюю	 
224	224	01.07.2021 18:31:00	Розр	ParseDecodeData	Мал	Ініціюю	 
225	225	01.07.2021 18:31:00	Розр	ParseDecodeData	Онл	Ініціюю	 
226	226	01.07.2021 18:31:00	Розр	ParseDecodeData	Web	Ініціюю	 
227	227	01.07.2021 18:31:00	Розр	DecodeAction	Розр	Ініціюю	 
228	228	01.07.2021 18:31:00	Розр	DecodeAction	Вір	Ініціюю	 
229	229	01.07.2021 18:31:00	Розр	DecodeAction	Мал	Ініціюю	 
230	230	01.07.2021 18:31:00	Розр	DecodeAction	Онл	Ініціюю	 
231	231	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
232	232	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
233	233	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
234	234	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
235	235	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
236	236	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
237	237	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
238	238	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
239	239	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
240	240	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
241	241	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
242	242	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
243	243	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
244	244	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
245	245	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
246	246	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
247	247	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
248	248	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
249	249	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
250	250	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
251	251	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
252	252	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
253	253	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
254	254	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
255	255	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
256	256	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
257	257	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
258	258	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
259	259	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
260	260	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
261	261	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
262	262	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
263	263	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
264	264	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
265	265	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
266	266	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
267	267	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
268	268	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
269	269	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
270	270	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
271	271	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
272	272	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
273	273	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
274	274	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
275	275	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
276	276	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
277	277	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
278	278	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
279	279	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
280	280	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
281	281	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
282	282	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	 
283	283	01.07.2021 18:30:00	Розр	DecodeAction	Web	Ініціюю	 
284	284	01.07.2021 18:30:00	Розр	ParseDecodeData	Розр	Ініціюю	 
285	285	01.07.2021 18:30:00	Розр	ParseDecodeData	Вір	Ініціюю	 
286	286	01.07.2021 18:30:00	Розр	ParseDecodeData	Мал	Ініціюю	 
287	287	01.07.2021 18:30:00	Розр	ParseDecodeData	Онл	Ініціюю	 
288	288	01.07.2021 18:30:00	Розр	ParseDecodeData	Web	Ініціюю	 
289	289	01.07.2021 18:30:00	Розр	DecodeAction	Розр	Ініціюю	 
290	290	01.07.2021 18:30:00	Розр	DecodeAction	Вір	Ініціюю	 
291	291	01.07.2021 18:30:00	Розр	DecodeAction	Мал	Ініціюю	 
292	292	01.07.2021 18:30:00	Розр	DecodeAction	Онл	Ініціюю	<img alt="Edit icon" data-bbox="838