

Содержание

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

19 Законный перехват

Разбор трафика

Оборудование

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

Конфигурация оборудования для разбора трафика:

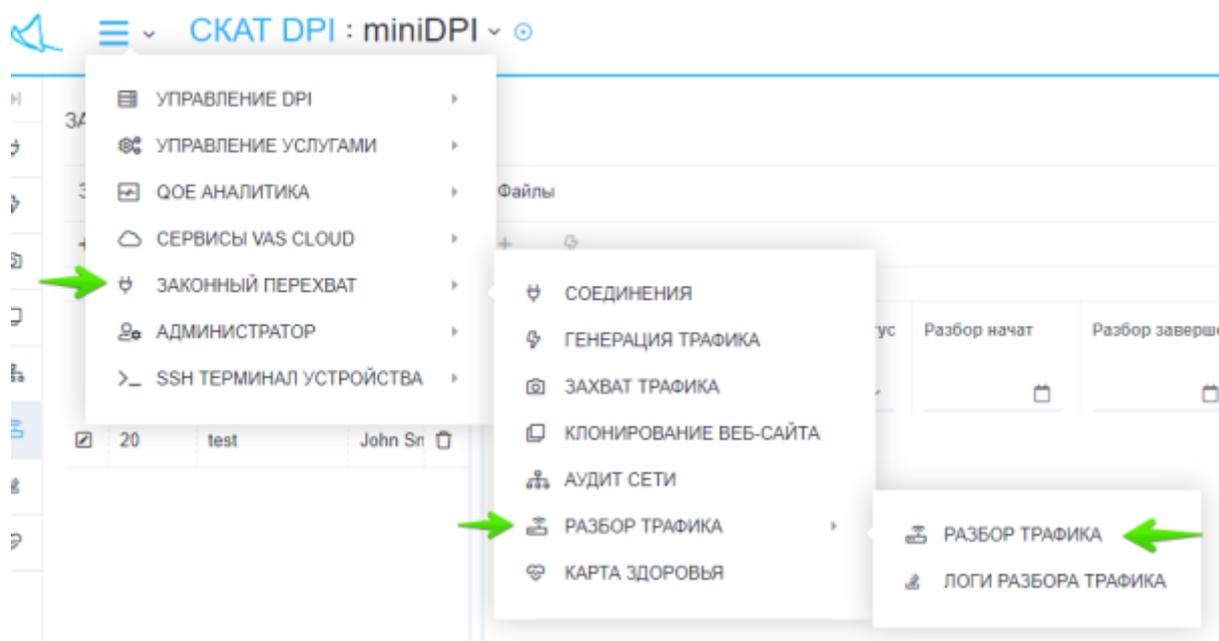
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

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.

Задачи

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

Создание задачи

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

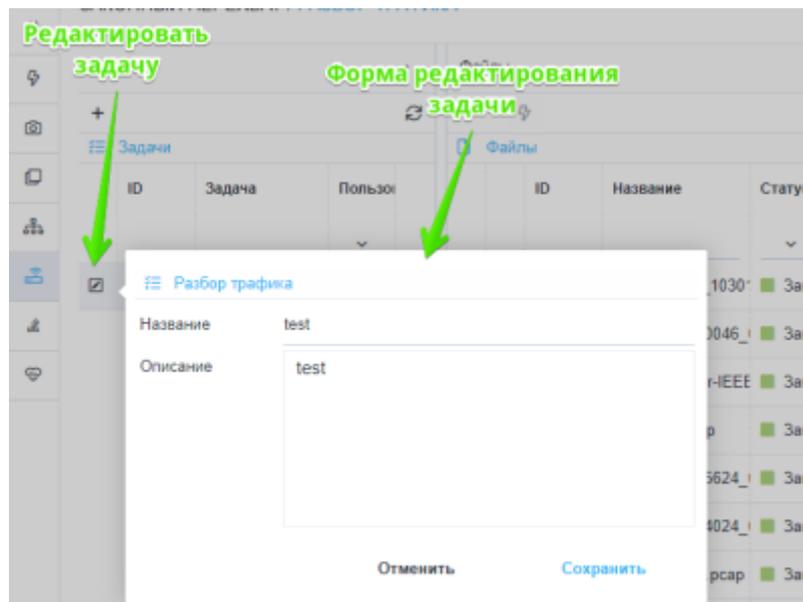
В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.



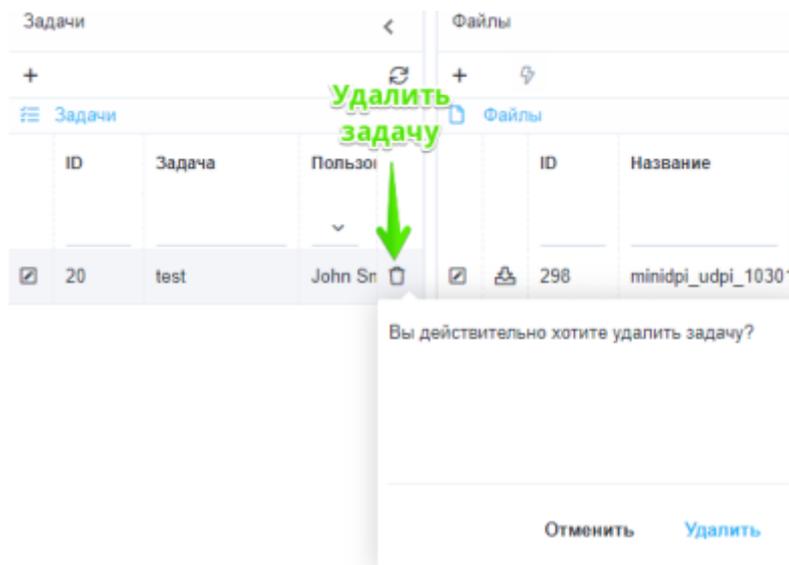
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

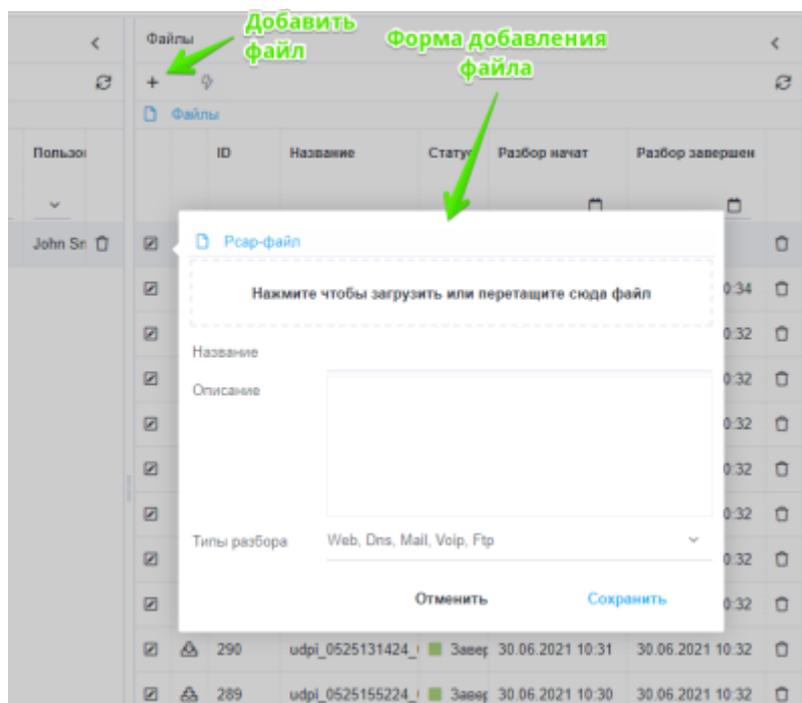


Файлы

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

Добавление файла

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



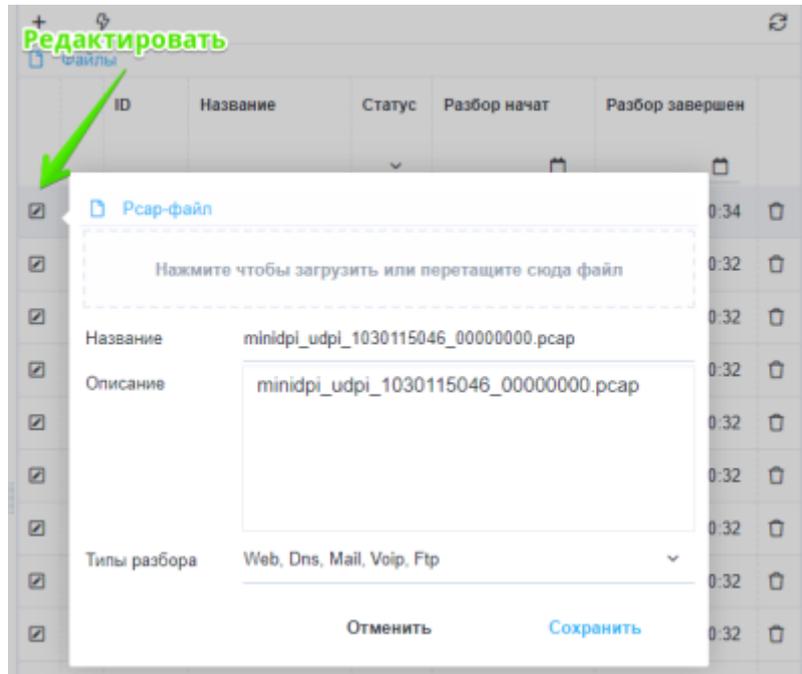
В открывшейся форме добавления файла:

- 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:

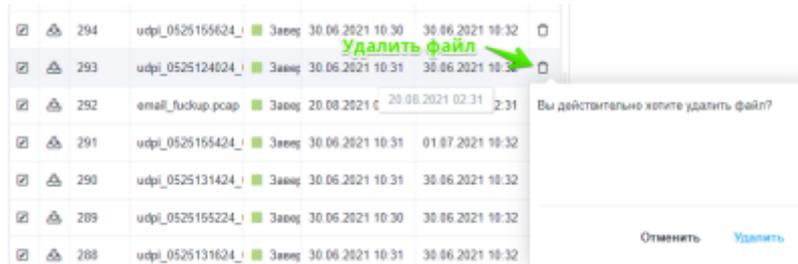
- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

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

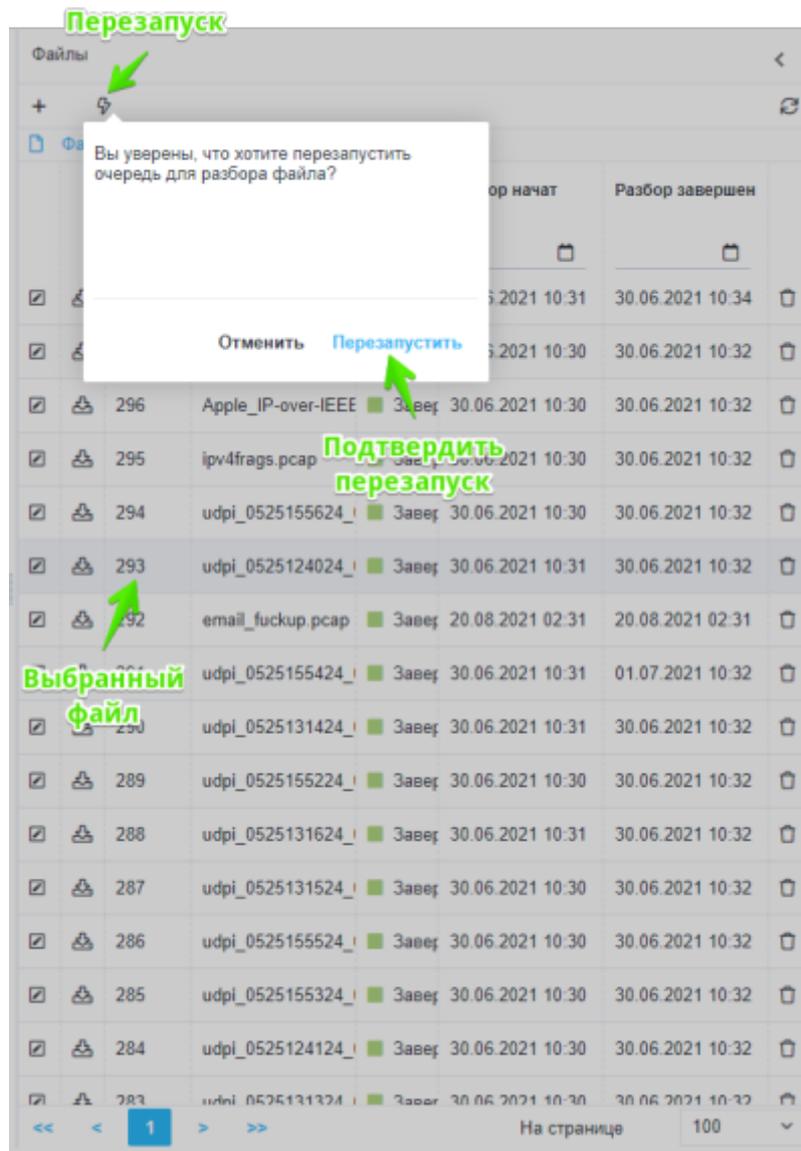
Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.



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.



Импорт файлов из раздела захвата трафика

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

- Адрес запроса
- Размер ответа в байтах
- Метод

Результаты

Web (49) Dns (55) Mail (1) Voip (0) Ftp (35)

Декодированные веб-элементы

Запросы Изображения

Дата	Урл	Размер	Метод	
30.10.2020 08:54:00	ocsp.pki.goog/gts1o1core	472	GET	?
30.10.2020 08:53:00	ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl_cab?bf757d	0	GET	?
30.10.2020 08:53:00	ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl_cab?261fc1	0	GET	?
30.10.2020 08:52:00	ocsp.digicert.com/	279	GET	?
30.10.2020 08:51:00	en.kremlin.ru/events/president/news	0	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/photo.svg	280	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/video.svg	347	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/big_text.svg	210	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/small_text.svg	225	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/medium_text.svg	224	GET	?
30.10.2020 08:51:00	en.kremlin.ru/events/president/news/calendar/2020	0:31	GET	?
30.10.2020 08:51:00	en.kremlin.ru/structure/president/standart	0	GET	?
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/Ty6y5wbIsAqJR47S3O9Rju5bxiEBuKA	388035	GET	?
30.10.2020 08:51:00	static.kremlin.ru/media/events/presidents/medium/y9GgT364rwY.jpg	55126	GET	?

На странице 100

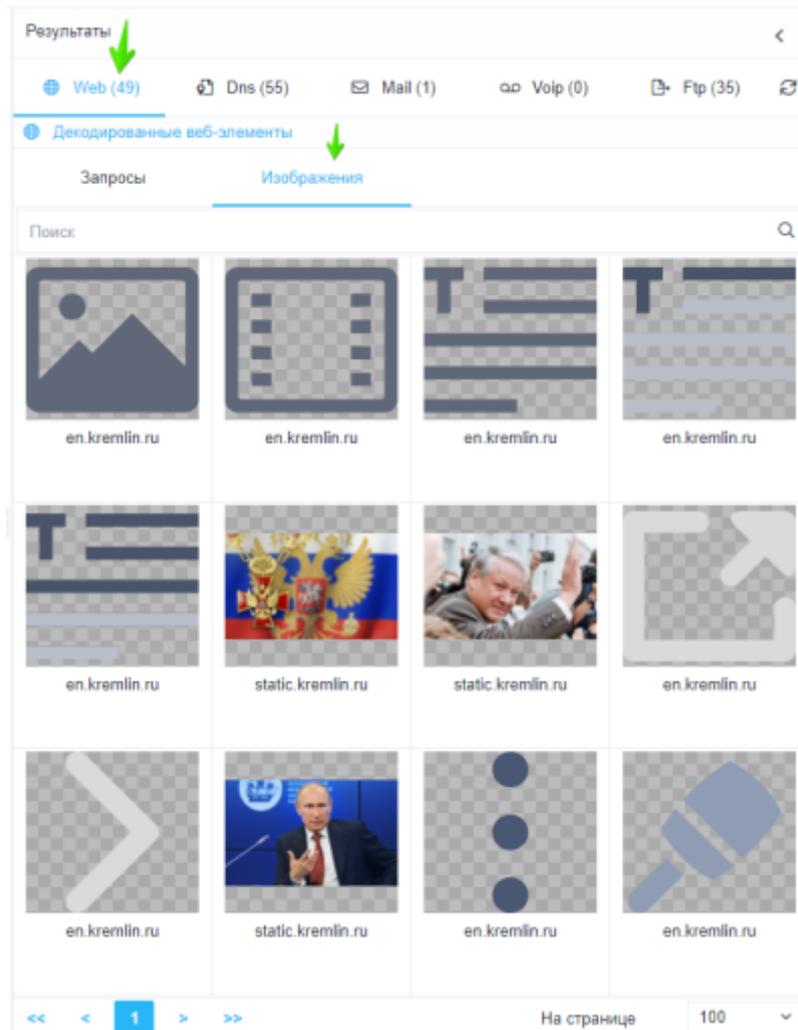
При нажатии на кнопку "Дополнительная информация о запросе"(?) откроется попап с дополнительной информацией о запросе:

- Агент
- Хост
- Урл
- Тип содержимого
- Кодировка
- Метод запроса
- Код ответа
- Размер ответа в байтах
- Порт отправителя
- Порт получателя
- Время TSP
- Протокол IP
- Версия IP

- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Идентификатор файла для разбора
- Имя файла для разбора
- Имя файла с содержимым ответа

Запросы		
Дата	Ураи	
30.10.2020 08:54:00	2090	
30.10.2020 08:53:00	2091	
30.10.2020 08:53:00	2092	
30.10.2020 08:52:00	2093	
30.10.2020 08:51:00	2094	
30.10.2020 08:51:00	2095	
30.10.2020 08:51:00	2096	
30.10.2020 08:51:00	2097	
30.10.2020 08:51:00	2098	
30.10.2020 08:51:00	2099	
30.10.2020 08:51:00	2100	
30.10.2020 08:51:00	2101	
30.10.2020 08:51:00	2102	
30.10.2020 08:51:00	2103	
30.10.2020 08:51:00	2104	
30.10.2020 08:51:00	2105	
30.10.2020 08:51:00	2106	
30.10.2020 08:51:00	2107	
30.10.2020 08:51:00	2108	
30.10.2020 08:51:00	2109	
30.10.2020 08:51:00	2110	
30.10.2020 08:51:00	2111	
30.10.2020 08:51:00	2112	
30.10.2020 08:51:00	2113	
30.10.2020 08:51:00	2114	
30.10.2020 08:51:00	2115	
30.10.2020 08:51:00	2116	
30.10.2020 08:51:00	2117	
30.10.2020 08:51:00	2118	
30.10.2020 08:51:00	2119	
30.10.2020 08:51:00	2120	
30.10.2020 08:51:00	2121	
30.10.2020 08:51:00	2122	
30.10.2020 08:51:00	2123	
30.10.2020 08:51:00	2124	
30.10.2020 08:51:00	2125	
30.10.2020 08:51:00	2126	
30.10.2020 08:51:00	2127	
30.10.2020 08:51:00	2128	
30.10.2020 08:51:00	2129	
30.10.2020 08:51:00	2130	
30.10.2020 08:51:00	2131	
30.10.2020 08:51:00	2132	
30.10.2020 08:51:00	2133	
30.10.2020 08:51:00	2134	
30.10.2020 08:51:00	2135	
30.10.2020 08:51:00	2136	
30.10.2020 08:51:00	2137	
30.10.2020 08:51:00	2138	
30.10.2020 08:51:00	2139	
30.10.2020 08:51:00	2140	
30.10.2020 08:51:00	2141	
30.10.2020 08:51:00	2142	
30.10.2020 08:51:00	2143	
30.10.2020 08:51:00	2144	
30.10.2020 08:51:00	2145	
30.10.2020 08:51:00	2146	
30.10.2020 08:51:00	2147	
30.10.2020 08:51:00	2148	
30.10.2020 08:51:00	2149	
30.10.2020 08:51:00	2150	
30.10.2020 08:51:00	2151	
30.10.2020 08:51:00	2152	
30.10.2020 08:51:00	2153	
30.10.2020 08:51:00	2154	
30.10.2020 08:51:00	2155	
30.10.2020 08:51:00	2156	
30.10.2020 08:51:00	2157	
30.10.2020 08:51:00	2158	
30.10.2020 08:51:00	2159	
30.10.2020 08:51:00	2160	
30.10.2020 08:51:00	2161	
30.10.2020 08:51:00	2162	
30.10.2020 08:51:00	2163	
30.10.2020 08:51:00	2164	
30.10.2020 08:51:00	2165	
30.10.2020 08:51:00	2166	
30.10.2020 08:51:00	2167	
30.10.2020 08:51:00	2168	
30.10.2020 08:51:00	2169	
30.10.2020 08:51:00	2170	
30.10.2020 08:51:00	2171	
30.10.2020 08:51:00	2172	
30.10.2020 08:51:00	2173	
30.10.2020 08:51:00	2174	
30.10.2020 08:51:00	2175	
30.10.2020 08:51:00	2176	
30.10.2020 08:51:00	2177	
30.10.2020 08:51:00	2178	
30.10.2020 08:51:00	2179	
30.10.2020 08:51:00	2180	
30.10.2020 08:51:00	2181	
30.10.2020 08:51:00	2182	
30.10.2020 08:51:00	2183	
30.10.2020 08:51:00	2184	
30.10.2020 08:51:00	2185	
30.10.2020 08:51:00	2186	
30.10.2020 08:51:00	2187	
30.10.2020 08:51:00	2188	
30.10.2020 08:51:00	2189	
30.10.2020 08:51:00	2190	
30.10.2020 08:51:00	2191	
30.10.2020 08:51:00	2192	
30.10.2020 08:51:00	2193	
30.10.2020 08:51:00	2194	
30.10.2020 08:51:00	2195	
30.10.2020 08:51:00	2196	
30.10.2020 08:51:00	2197	
30.10.2020 08:51:00	2198	
30.10.2020 08:51:00	2199	
30.10.2020 08:51:00	2200	

Во вкладке "Изображения" отображаются запросы, в ответ на которые возвращались изображения.



DNS

На вкладке результатов разбора DNS отображаются хосты.

В таблице доступны следующие данные:

- Дата и время запроса
- Хост

Результаты

Web (49) DNS (55) Mail (1) Voip (0) Ftp (35)

Детализированные данные DNS

Дата	Хост	
30.10.2020 08:54:00	iecvlist.microsoft.com	ⓘ
30.10.2020 08:54:00	sb-esl.google.com	ⓘ
30.10.2020 08:54:00	ocsp.pki.goog	ⓘ
30.10.2020 08:54:00	pki-goog.l.google.com	ⓘ
30.10.2020 08:54:00	sb-esl.google.com	ⓘ
30.10.2020 08:54:00	pki-goog.l.google.com	ⓘ
30.10.2020 08:53:00	ctfd.windowsupdate.com	ⓘ
30.10.2020 08:53:00	ctfd.windowsupdate.com	ⓘ
30.10.2020 08:53:00	ctfd.windowsupdate.com	ⓘ
30.10.2020 08:53:00	DESKTOP-H465JAS.local	ⓘ
30.10.2020 08:52:00	windows.policies.live.net	ⓘ
30.10.2020 08:52:00	windows.policies.live.net	ⓘ

Дополнительная информация о запросе

На странице 100

При нажатии на кнопку "Дополнительная информация о запросе"(?) откроется попап с дополнительной информацией о запросе:

- Список хостов
- Список адресов
- Список сертификатов
- Дата запроса
- Время ответа
- Порт отправителя
- Порт получателя
- Протокол IP
- Версия IP
- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Идентификатор запроса
- Идентификатор файла для разбора
- Имя файла для разбора

Результаты

Web (49) DNS (55) Mail (1) Voip (0) Ftp (35)

✓ Детализированные данные DNS

Дата	Хост
30.10.2020 08:54:00	ie9vta
30.10.2020 08:54:00	sb-sa
30.10.2020 08:54:00	osarj
30.10.2020 08:54:00	pkj-ga
30.10.2020 08:54:00	sb-sa
30.10.2020 08:53:00	pkj-ga
30.10.2020 08:53:00	ctel v
30.10.2020 08:53:00	ctel v
30.10.2020 08:53:00	ctel v
30.10.2020 08:53:00	DESK
30.10.2020 08:52:00	winfo
30.10.2020 08:52:00	winfo

Информация о DNS

Ключ	Значение
Хост 2	ie9comview.vo.mssecnd.net
Хост 3	cs9.wpc.v0cdn.net
Адрес	152.199.19.161
Сертификат 1	ie9comview.vo.mssecnd.net
Сертификат 2	cs9.wpc.v0cdn.net

Информация о запросе

Eth	
Тип Eth	0x00000000
Eth отправитель	68:1d:ef:14:1d:d2
Eth получатель	4c:5e:0c:f3:48:58

Файл

ID записи	4433
ID файла	298
Имя файла	miniip_udp_1030115846_00000000.pcap

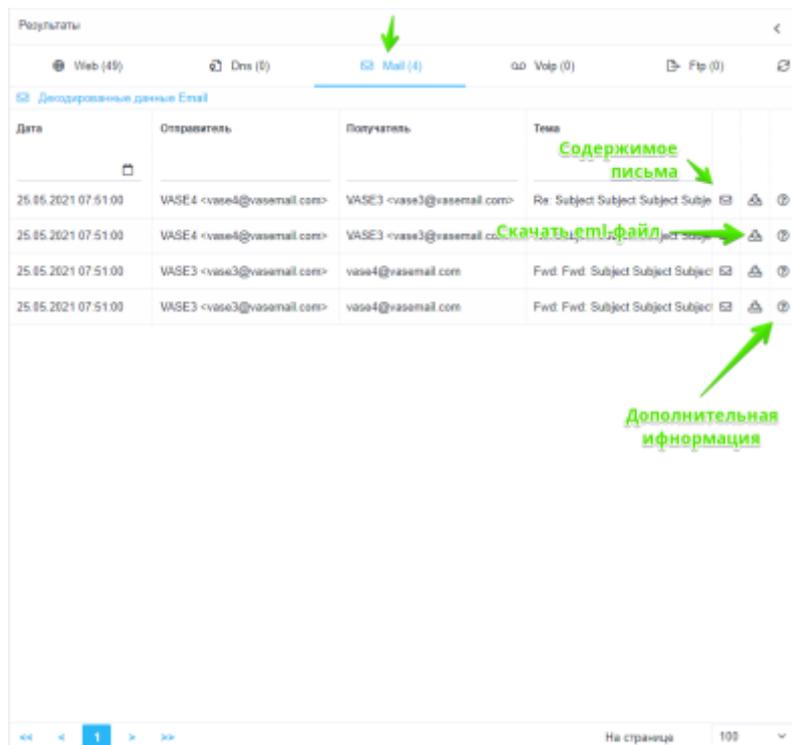
Закрыть

Mail

На вкладке результатов разбора MAIL отправленные/полученные Email-ы.

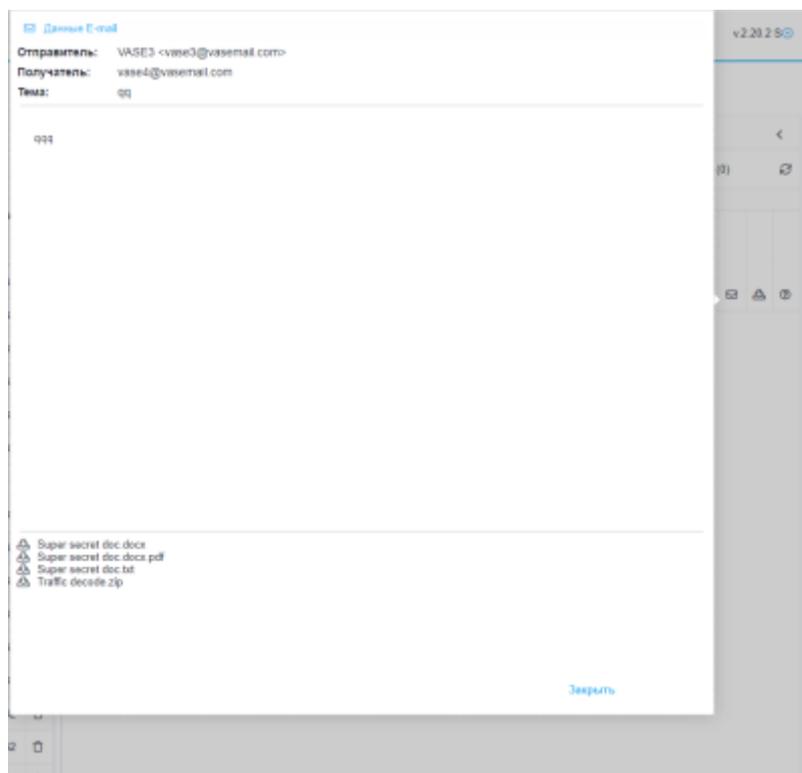
В таблице доступны следующие данные:

- Дата и время отправки/получения;
- Отправитель
- Получатель
- Тема письма



При нажатии на кнопку Содержимого письма откроется попап в котором доступны:

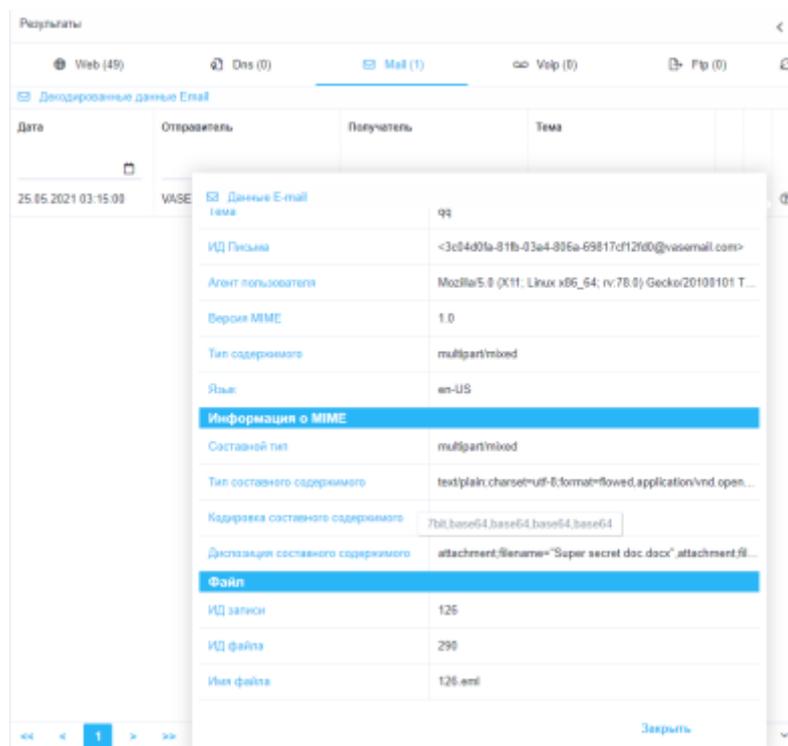
- Отправитель
- Получатель
- Тема письма
- Текст письма
- Список приложенных файлов к письму (можно скачать)



При нажатии на кнопку Дополнительной информации(?) откроется попап с дополнительной

информацией о письме:

- Порт отправителя
- Порт получателя
- Протокол IP
- Версия IP
- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Отправитель
- Получатель
- Тема
- Идентификатор письма
- Агент пользователя
- Версия MIME
- Тип содержимого
- Язык
- Составной тип
- Тип составного содержимого
- Кодировка составного содержимого
- Диспозиция составного содержимого
- Идентификатор записи
- Идентификатор файла для разбора
- Имя Eml-файла



Voip

В разработке.

Ftp

На вкладке результатов разбора FTP отображаются файлы отправленные/полученные посредством FTP.

В таблице доступны следующие данные:

- Дата и время запроса
- Имя файла
- Направление (Скачивание/Загрузка)
- Размер файла в байтах
- Адрес клиента
- Адрес сервера

Дата	Файл	Направление	Размер	Клиент	Сервер
30.10.2020 08:52:00	stojka_image.zip	Скачивание	5234345	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	Pantone.tcl	Скачивание	28	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	e-link_logo_image.zip	Скачивание	258678	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	DIR_300_B1_image.HiSide_OOBE\lslf	Скачивание	24693932	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	DIR_300_B1_image.HiSide_OOBE\lslfd	Скачивание	14822229	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	desktop.ini	Скачивание	380	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	sab.jpg	Скачивание	98942	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	kancsher.jpg	Скачивание	127441	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	peripheral.jpg	Скачивание	111157	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	images.zip	Скачивание	2529758	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	pccard.jpg	Скачивание	148707	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	eflca.jpg	Скачивание	130091	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	network.jpg	Скачивание	148619	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	modern.jpg	Скачивание	138187	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	Transceiver.jpg	Скачивание	269790	192.168.88.13	178.170.168.19

При нажатии на кнопку "Дополнительная информация" (?) откроется попап с дополнительной информацией о запросе:

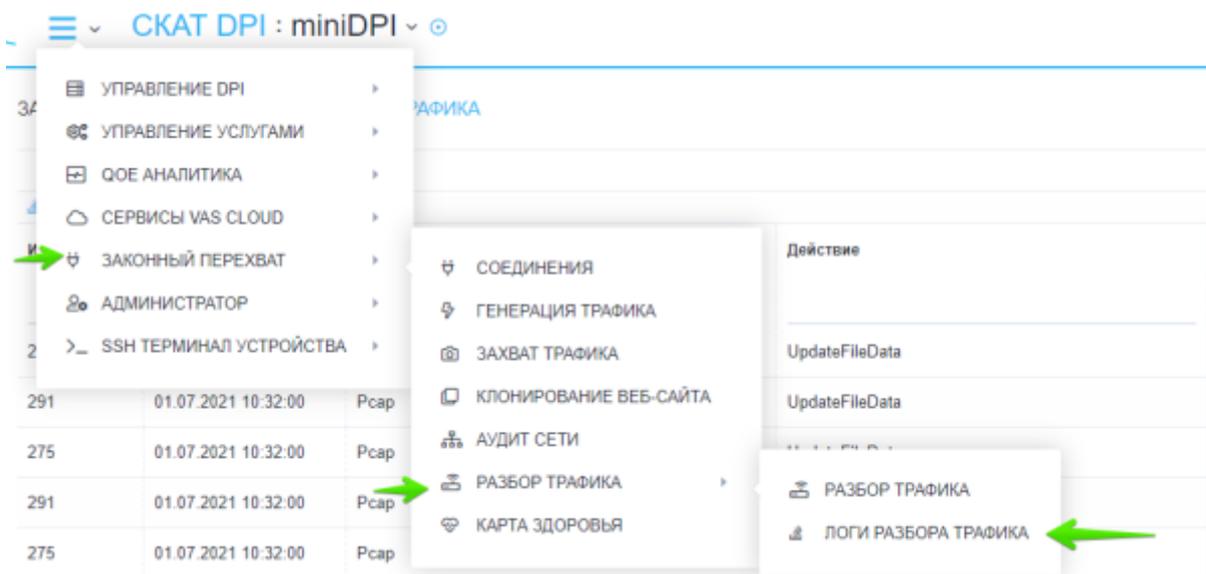
- Порт отправителя
- Порт получателя
- Протокол IP
- Версия IP
- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Имя файла
- Директория Ftp
- Размер файла в байтах
- Направление

- Идентификатор файла для разбора
- Файл ответа

Результаты		Информация Ftp	
Web (49)		Версия Ftp	4
Декодированные данные Ftp		Ftp отправителя	192.168.88.13
Дата		Ftp получателя	178.170.168.19
Файл		Eth	
30.10.2020 08:52:00	stolka_lo	Тип Eth	0x00000000
30.10.2020 08:52:00	Рантонс	Eth отправителя	68:1d:ef:14:1d:d2
30.10.2020 08:52:00	link_lo	Eth получателя	4c:5e:0c:f3:48:58
30.10.2020 08:52:00	DIR_300	Информация Ftp	
30.10.2020 08:52:00	DIR_300	Имя файла	transceiver.jpg
30.10.2020 08:52:00	stolka_lo	Директория Ftp	/pub/Images/CON
30.10.2020 08:52:00	ssh.jpg	Размер файла (байты)	127441
30.10.2020 08:52:00	transce	Направление	Скачивание
		Файл	
		ИД файла	250
		Файл ответа	wYCWtNgy0r:transceiver.jpg

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.

ЗАКОННЫЙ ПЕРЕХВАТ / ЛОГИ РАБОТЫ ТРАФИКА

Обновить список задач

Операция перехвата трафика

Удалить задачу

ID Задачи	Дата	Тип	Действие	Тип трафика	Статус	Описание	
275	01.07.2021 18:32:00	Резерв	UpdateFileData	Резерв	Успешно		
291	01.07.2021 18:32:00	Резерв	UpdateFileData	Резерв	Успешно		
276	01.07.2021 18:32:00	Резерв	UpdateFileData	Вирт	Успешно		
301	01.07.2021 18:32:00	Резерв	ParseDecodedData	Резерв	Успешно		
275	01.07.2021 18:32:00	Резерв	UpdateFileData	Mail	Успешно		
275	01.07.2021 18:34:00	Резерв	UpdateFileData	Они	Успешно		
275	01.07.2021 18:34:00	Резерв	UpdateFileData	Web	Успешно		
275	01.07.2021 18:34:00	Резерв	ParseDecodedData	Резерв	Успешно		
275	01.07.2021 18:35:00	Резерв	ParseDecodedData	Вирт	Успешно		
275	01.07.2021 18:35:00	Резерв	ParseDecodedData	Mail	Успешно		
275	01.07.2021 18:35:00	Резерв	ParseDecodedData	Они	Успешно		
276	01.07.2021 18:35:00	Резерв	ParseDecodedData	Web	Успешно		
276	01.07.2021 18:35:00	Резерв	DecodeAction	Резерв	Успешно		
275	01.07.2021 18:35:00	Резерв	DecodeAction	Вирт	Успешно		
275	01.07.2021 18:36:00	Резерв	DecodeAction	Mail	Успешно		
275	01.07.2021 18:36:00	Резерв	DecodeAction	Они	Успешно		
276	01.07.2021 18:36:00	Резерв	DecodeAction	Web	Успешно		

Просмотр информации о задаче

Постраничный переход

Количество записей на странице