

Содержание

19 Законный перехват	3
<i>Разбор трафика</i>	3
Оборудование	3
Раздел	3
Логи разбора трафика	23

19 Законный перехват

- [Разбор трафика](#)

Разбор трафика

Оборудование

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

Конфигурация оборудования для разбора трафика:

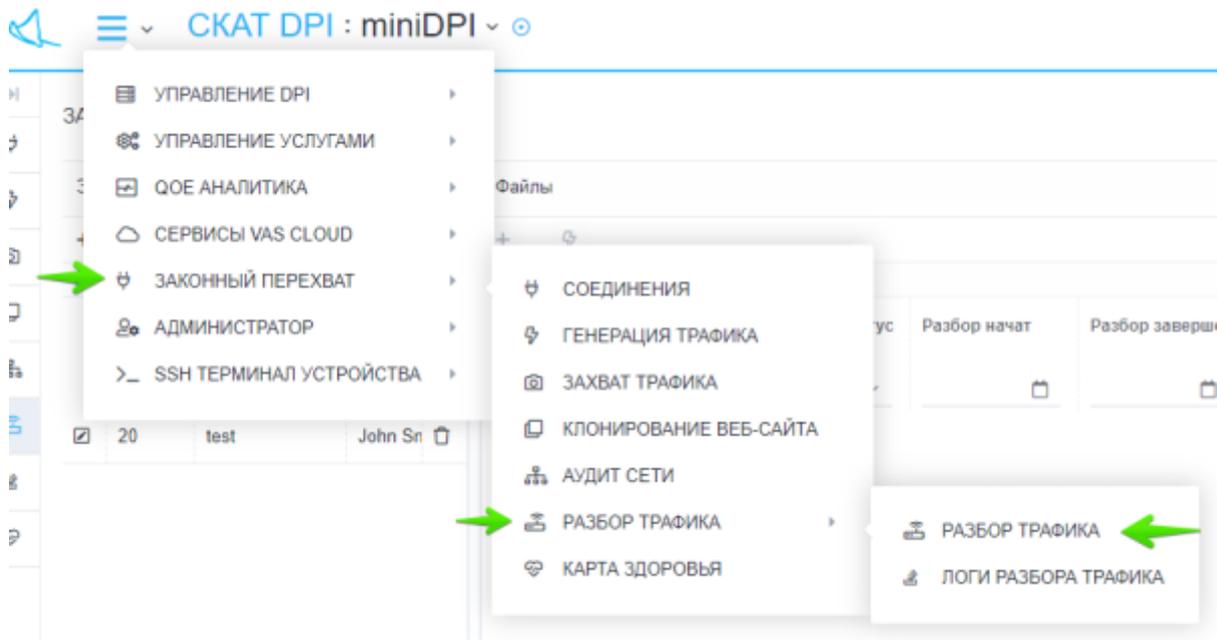
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

Для установки необходимых для работы утилит необходимо выполнить следующую команду:

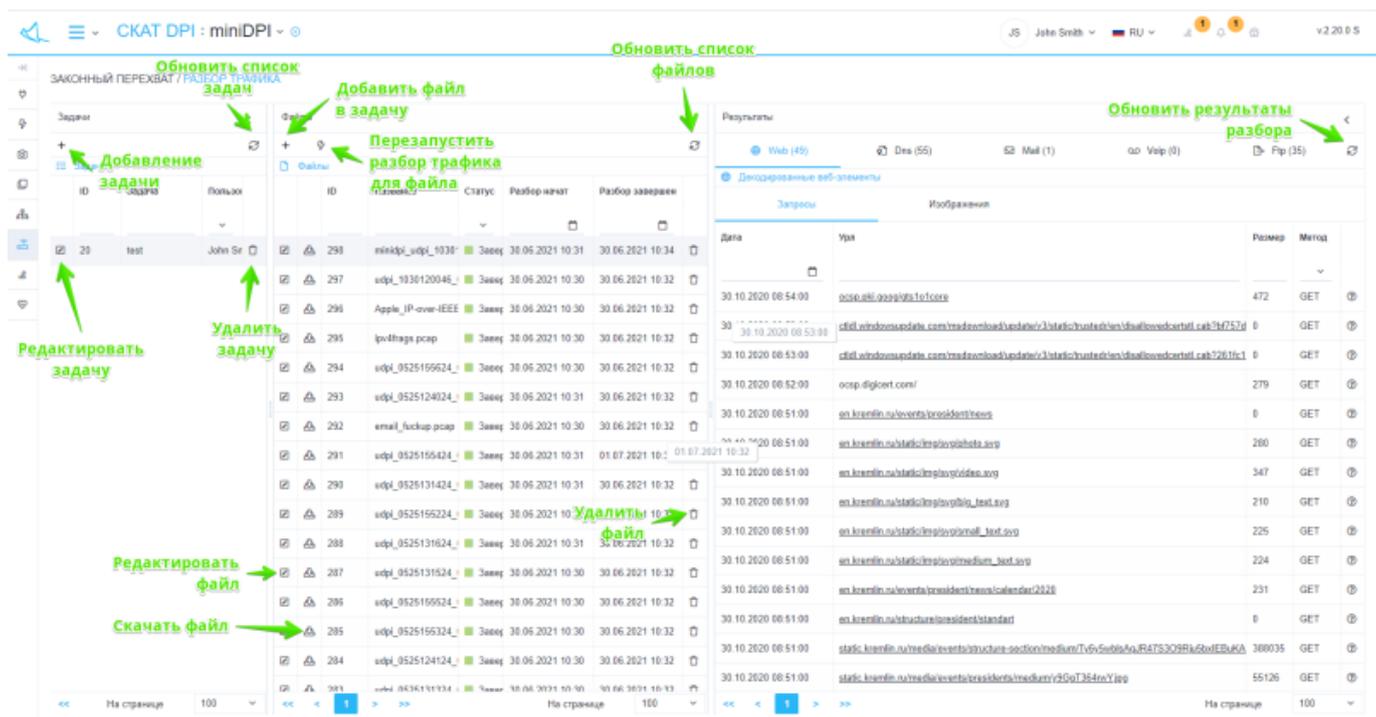
```
apt install wireshark tshark sox
```

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.

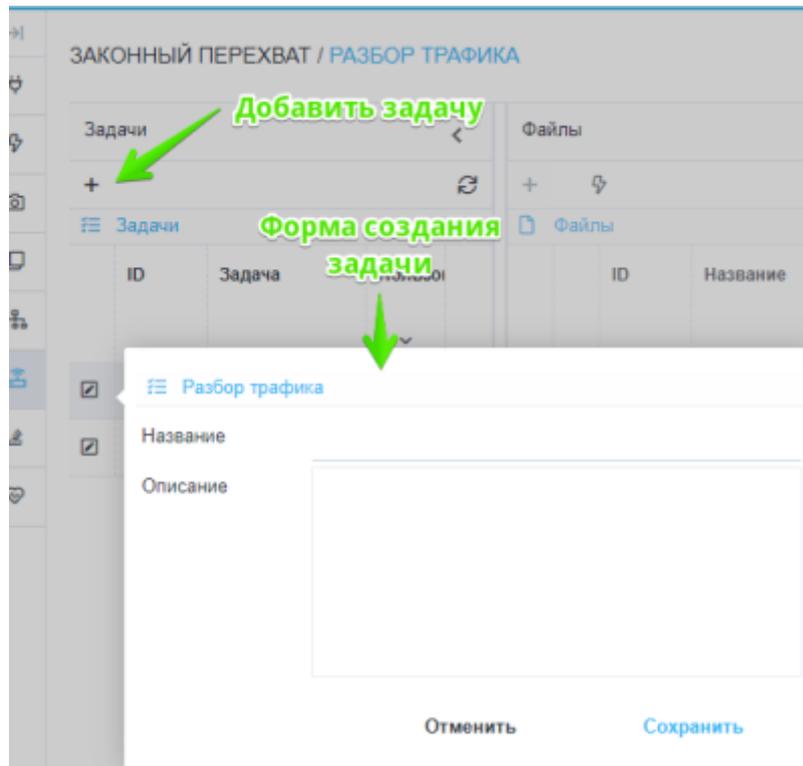


Задачи

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.



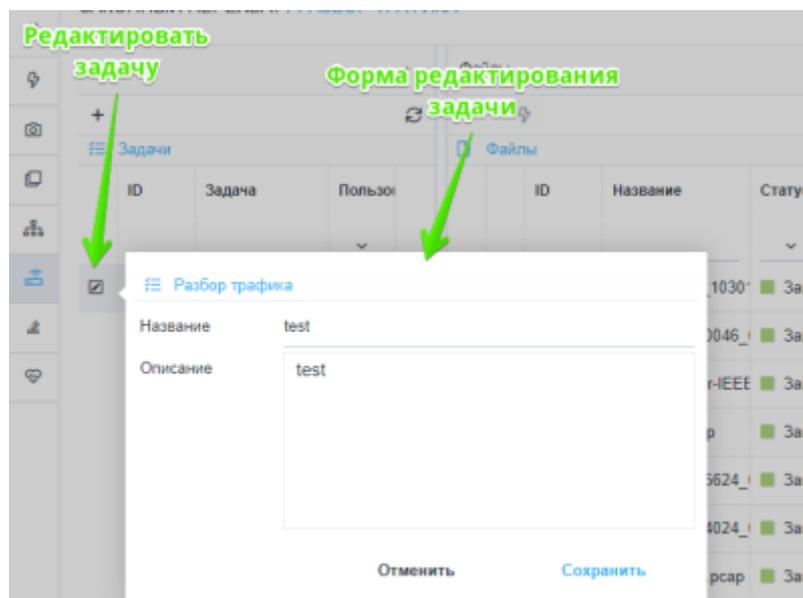
В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.



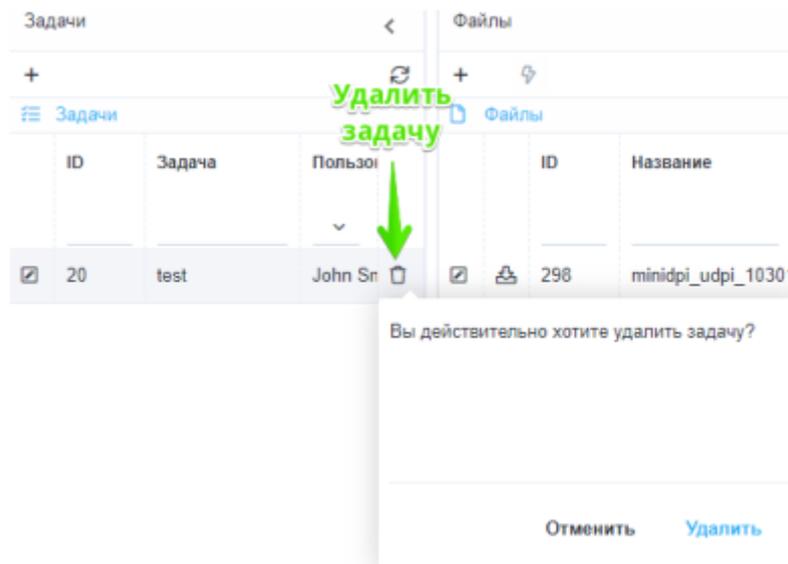
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

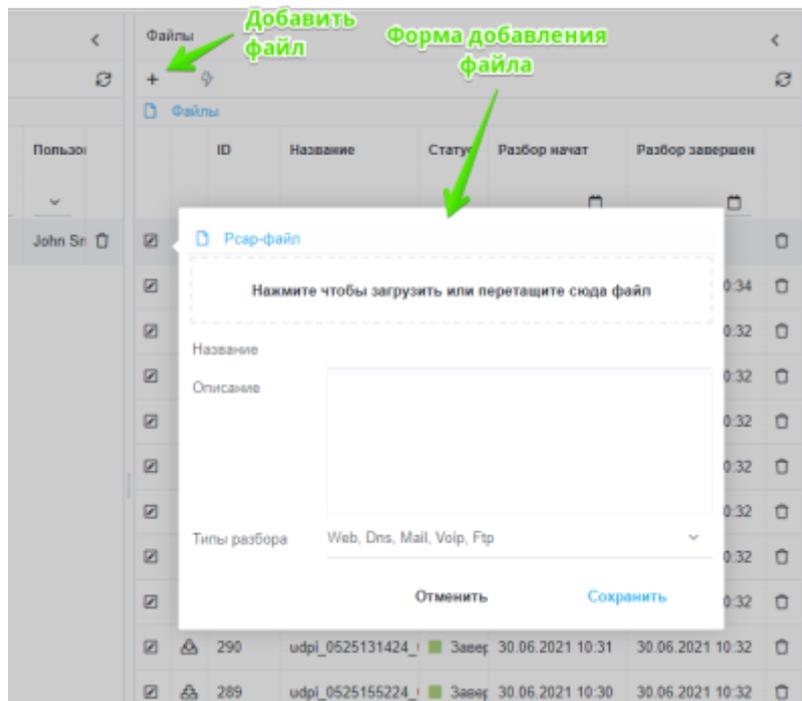


Файлы

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.



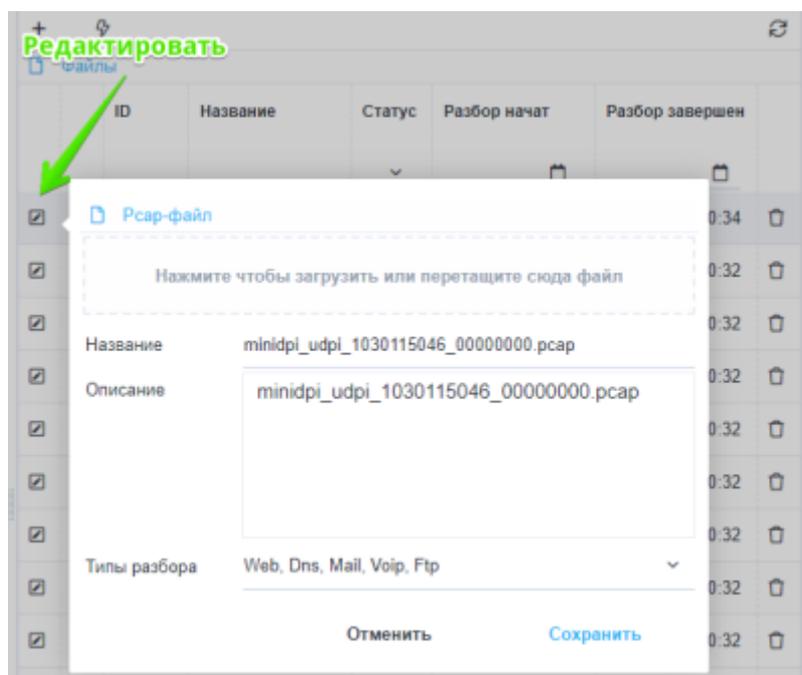
В открывшейся форме добавления файла:

- 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:

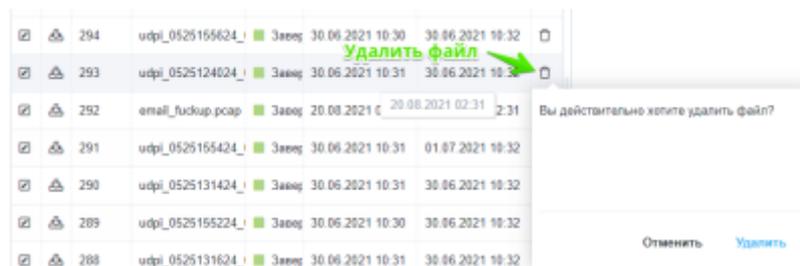
- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

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

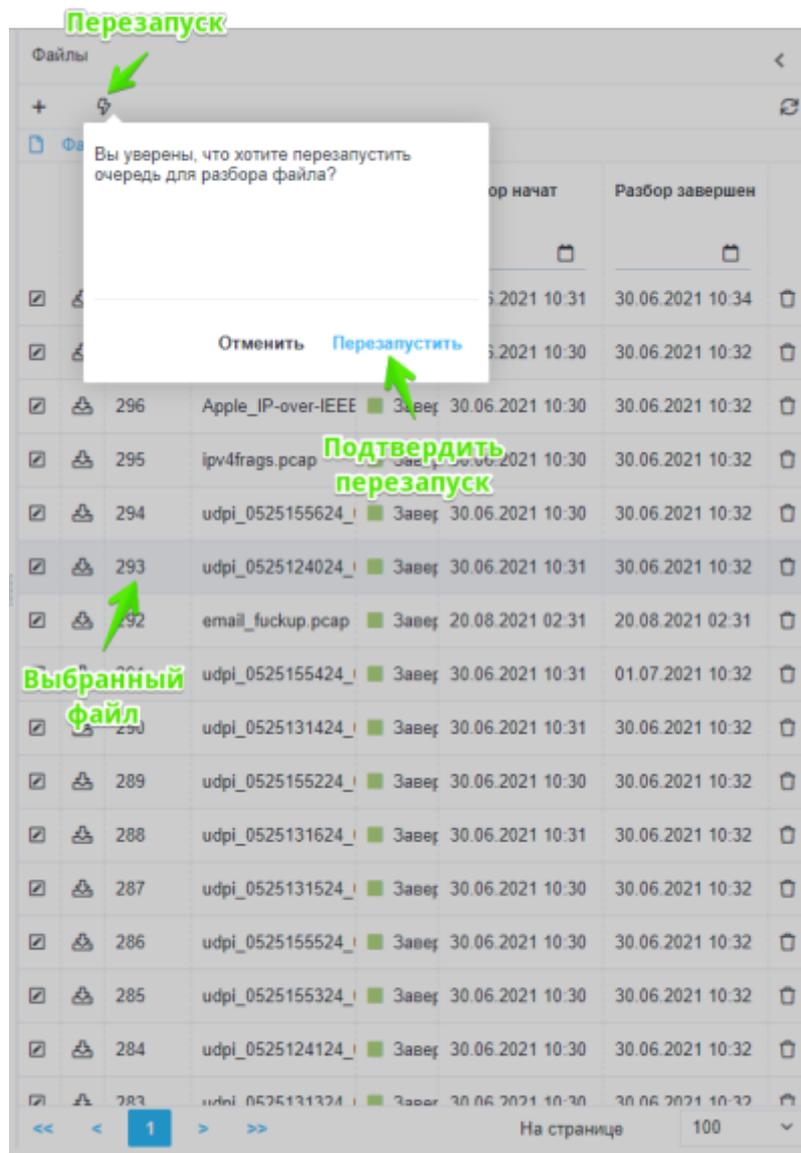
Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.



Перезапуск разбора файла

Для перезапуска разбора файла:

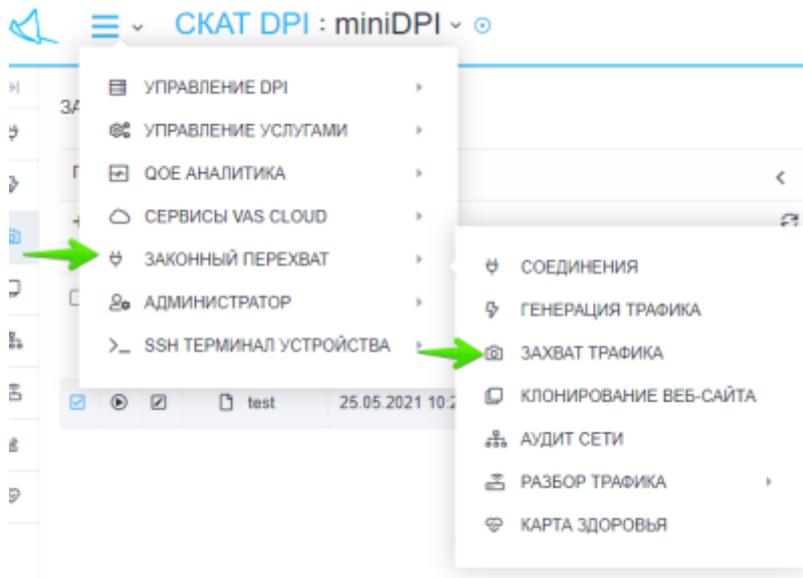
1. Выберите необходимый файл из списка;
2. Нажмите на кнопку перезапуска разбора в тулбаре;
3. Подтвердите либо отмените действие.



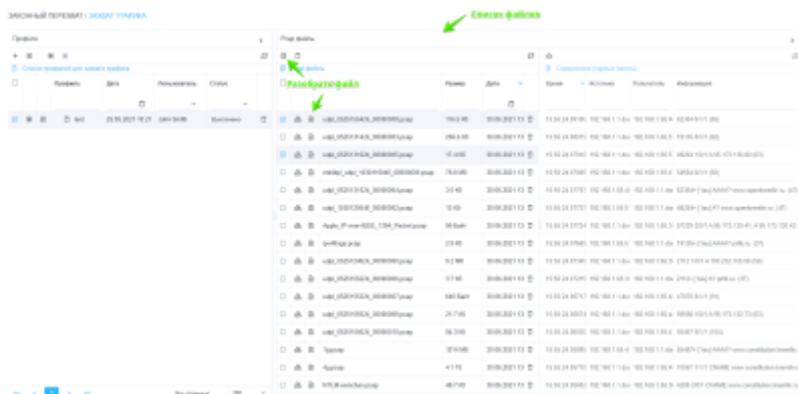
Импорт файлов из раздела захвата трафика

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

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

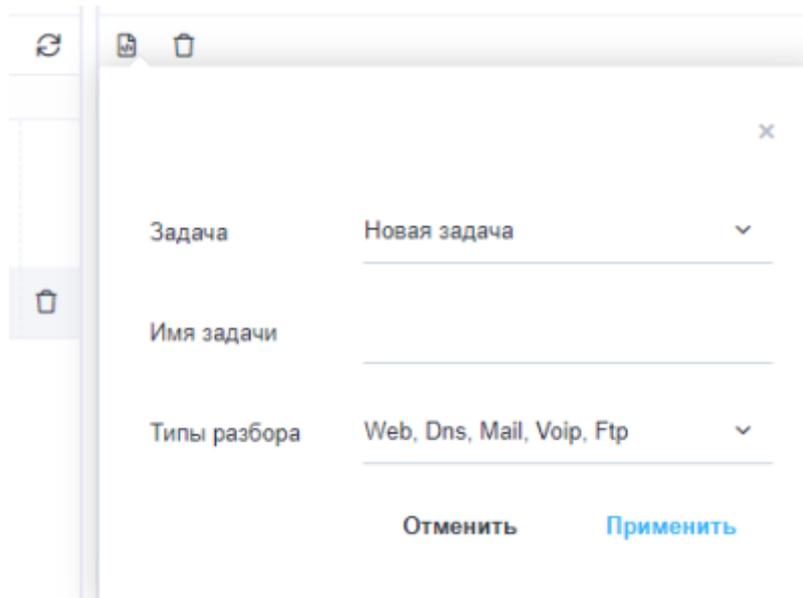


В списке файлов выберите файлы, которые необходимо разобрать и нажмите кнопку разбора.



В открывшейся форме:

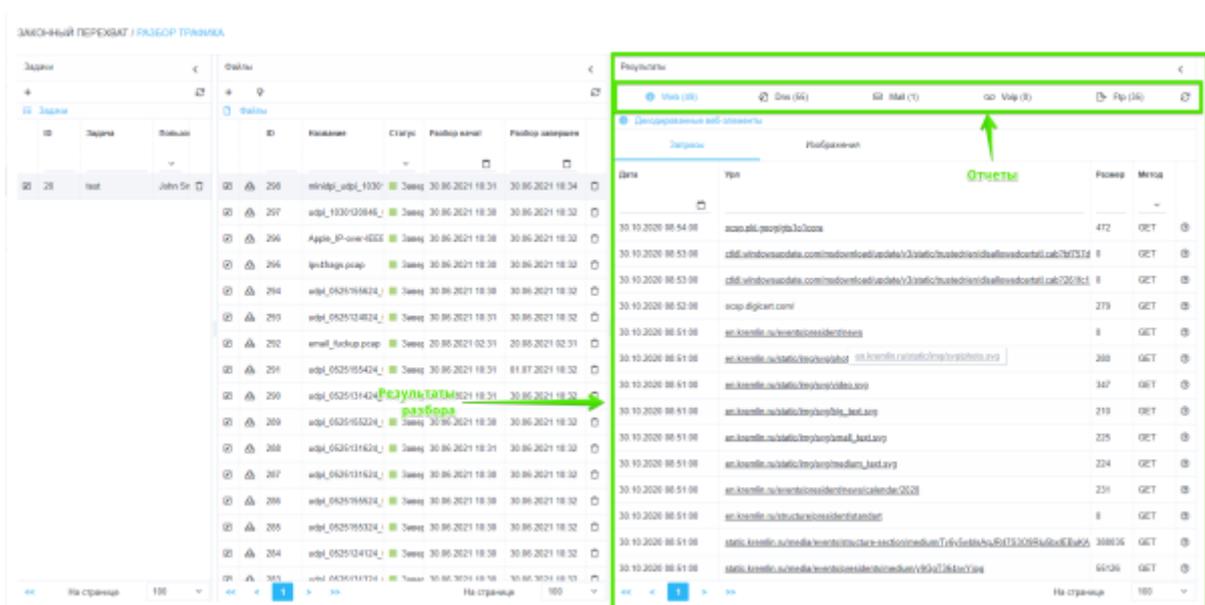
- Выберите задачу Разбора трафика, в которую будут импортированы файлы.
- В случае выбора "Новой задачи" - введите имя задачи, которая будет создана при импорте.
- Типы разбора для импортируемых файлов (Web,Dns,Mail,Voip,Ftp).



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

Результаты разбора

Результаты разбора находятся в правой части страницы Разбора трафика.



Web

На вкладке результатов разбора Web отображаются HTTP-запросы.

На вкладке "Запросы" отображаются "сырые" данные о запросах.

В таблице доступны следующие данные:

- Дата и время запроса

- Адрес запроса
- Размер ответа в байтах
- Метод

Результаты

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

Декодированные веб-элементы

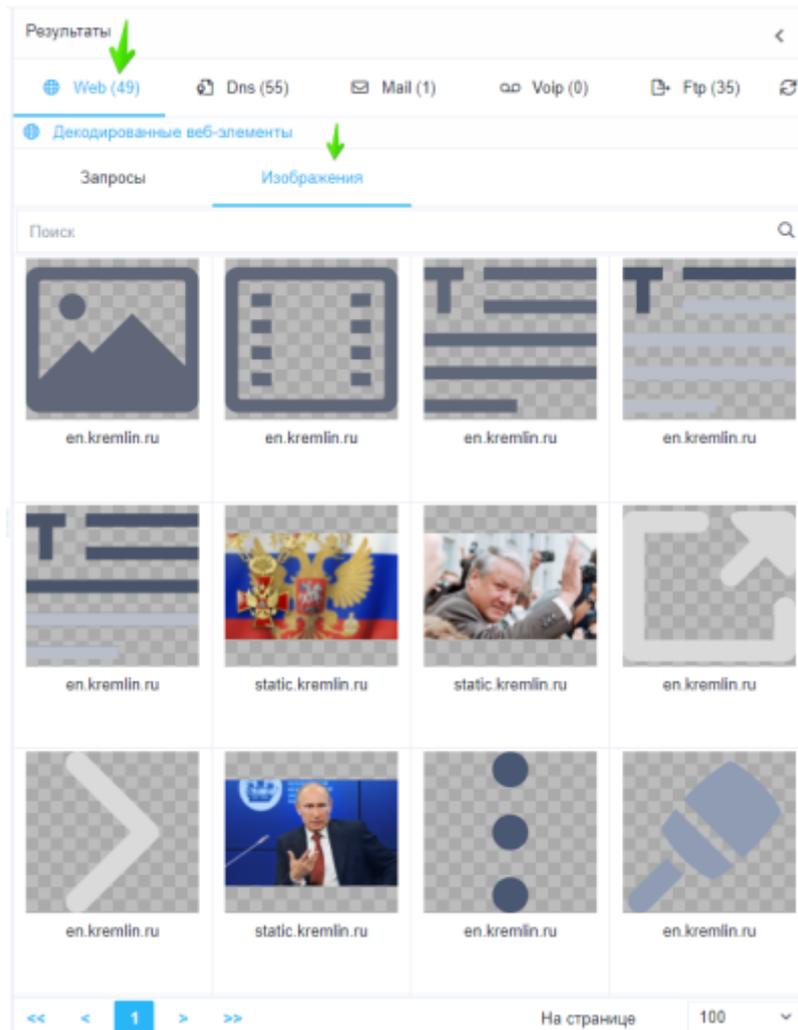
Запросы Изображения

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



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 записи
- 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

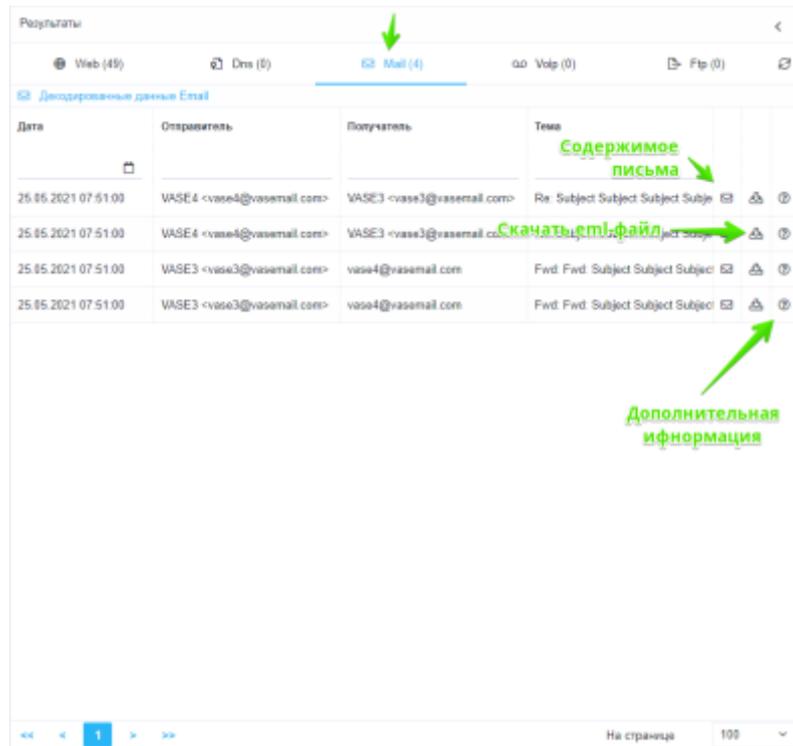
Закрыть

Mail

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

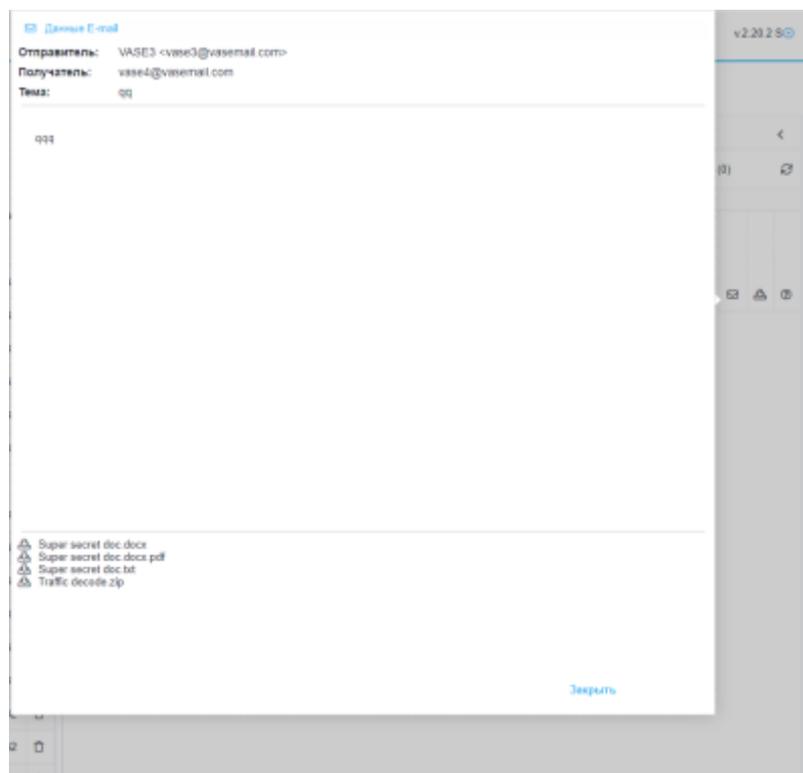
В таблице доступны следующие данные:

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



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

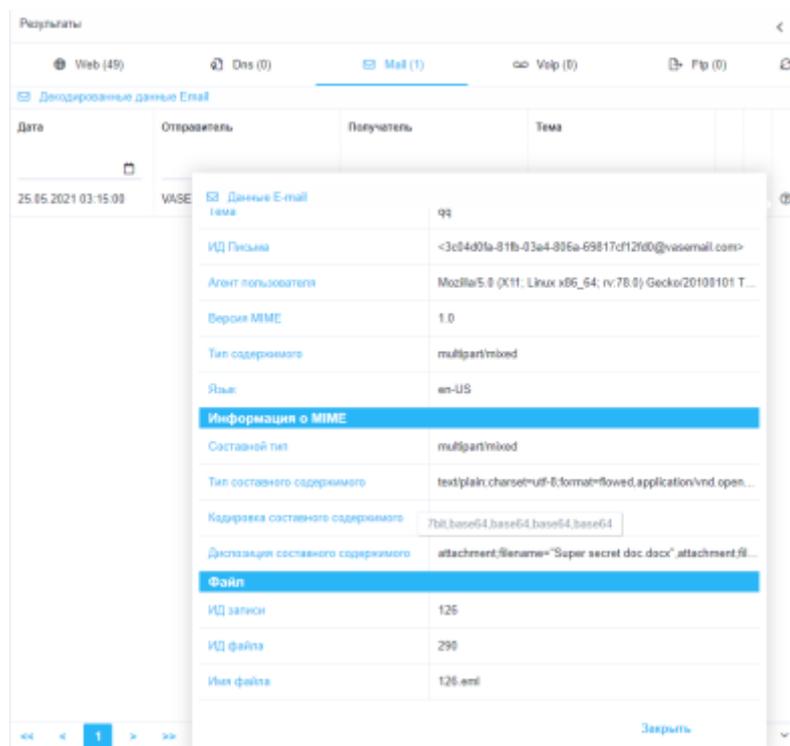
- Отправитель
- Получатель
- Тема письма
- Текст письма
- Список приложенных файлов к письму (можно скачать)



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

На вкладке результатов разбора Voip информация о совершенных Voip-сессиях.

В таблице доступны следующие данные:

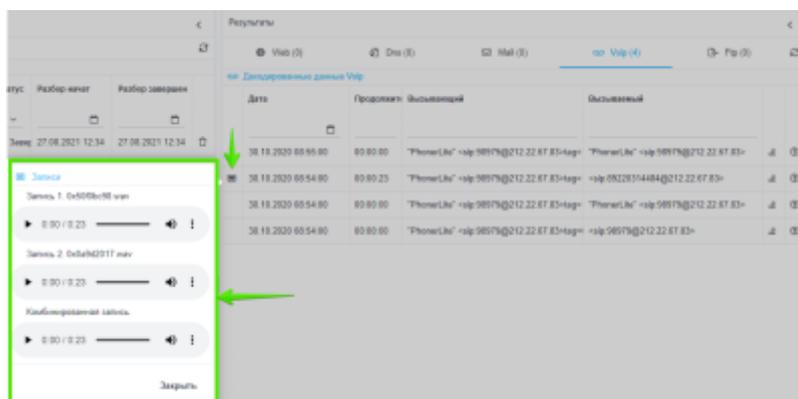
- Дата и время сессии
- Продолжительность сессии
- Вызывающий
- Вызываемый

The screenshot shows a table of VoIP call logs. The table has columns for Date, Duration, Caller, and Recipient. A green arrow points to the 'Voip (4)' filter. Another green arrow points to a 'Записи' (Records) button. A third green arrow points to a 'Логи запросов' (Request Logs) button. A fourth green arrow points to a 'Доступна аудиозапись' (Audio recording available) label. A fifth green arrow points to a 'Дополнительная информация' (Additional information) label.

Дата	Продолжит.	Вызывающий	Вызываемый		
30.10.2020 08:55:00	00:00:00	"PhonerLite" <sip:98979@212.22.67.83>tag=	"PhonerLite" <sip:98979@212.22.67.83>	↓	ⓘ
30.10.2020 08:54:00	00:00:23	"PhonerLite" <sip:98979@212.22.67.83>tag=	<sip:89220314404@212.22.67.83>	↓	ⓘ
30.10.2020 08:54:00	00:00:00	"PhonerLite" <sip:98979@212.22.67.83>tag=	"PhonerLite" <sip:98979@212.22.67.83>	↓	ⓘ
30.10.2020 08:54:00	00:00:00	"PhonerLite" <sip:98979@212.22.67.83>tag=	<sip:98979@212.22.67.83>	↓	ⓘ

При нажатии на кнопку Записи откроется попап, в котором можно прослушать аудиозаписи:

- Вызывающего
- Вызываемого
- Комбинированную



При нажатии на кнопку Логи запросов откроется попап с логами всех запросов сессии.

Результаты

Web (0) Dns (0) Mail (0) **Voip (4)** Fp (0)

Детализированные данные Voip

Дата	Продолжит	Вызывающей	Вызываемый
30.10.2020 08:55:00	00:00:00	"PhonerLite" <sip:98979@212.22.67.83>;tag="PhonerLite"	<sip:98979@212.22.67.83>
30.10.2020 08:54:00			
30.10.2020 08:54:00			
30.10.2020 08:54:00			

Лог запроса

```

1 Via: SIP/2.0/UDP 192.168.88.13:5060;branch=c9b54b40548532fb18b11aceabcb3f6e2
2 From: "PhonerLite" <sip:98979@212.22.67.83>;tag=122272390
3 To: <sip:98979@212.22.67.83>
4 Call-ID: 89548532-F818-E811-AC69-8CD9C3F0E28C@192.168.88.13
5 Cseq: 4 INVITE
6 Contact: <sip:98979@192.168.88.13:5060;gr=98CD712E-F818-E811-AC69-8CD9C3F0E28C>
7 Content-Type: application/sdp
8 Allow: INVITE, ACK, BYE, CANCEL, INFO, MESSAGE, NOTIFY, OPTIONS, REFER, UPDATE,
9 Max-Forwards: 70
10 User-Agent: PhonerLite 2.76
11 Session-Expires: 1800
12 Supported: 100rel, replaces, from-change, gruu, timer
13 P-Preferred-Identity: <sip:98979@212.22.67.83>
14 Content-Length: 346
15
16 s=0
17 m= 3787392535 1 IN IP4 192.168.88.13
18 s=PhonerLite 2.76
19 c=IN IP4 192.168.88.13
20 t=0 0
21 m=audio 5062 RTP/AVP 8 0 5 9 18 101
22 a=rtpmap:8 PCMA/8000

```

Закреть

На странице 100

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

- Порт отправителя
- Порт получателя
- Протокол
- Версия IP
- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Продолжительность сессии
- Вызывающий
- Вызываемый
- Идентификатор звонка
- Ssrc исходящий
- Ssrc входящий
- Названия файлов аудиозаписей
- Идентификатор файла для разбора

Информация Voip	
Eth отправителя	68:1d:ef:14:1d:d2
Eth получателя	4c:5e:0c:f3:48:58
Sip info	
Продолжительность	00:00:23
Вызывающий	"PhonerLite" <sip:98979@212.22.67.83>tag=122272309
Вызываемый	<sip:89220314484@212.22.67.83>
ID звонка	00540532-FB18-EB11-ACE9-BCD3C3F0E2BC@192.168.8...
Информация Rtp	
Ssrc от	0x50f0bc98
Ssrc к	0x0a9d2017
Запись 1	0x50f0bc98.wav
Запись 2	0x0a9d2017.wav
Комбинированная запись	0x50f0bc98_0x0a9d2017.wav
Файл	
ИД файла	321

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

Результаты

Web (49) Des (55) Mail (1) Vpn (8) Ftp (25)

Декодированные данные Ftp

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	Pastorena.txt	Скачивание	28	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	elink_login_image.zip	Скачивание	258678	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	DIR-300_B1_image.HiSide_OOBE\off	Скачивание	24693932	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	DIR-300_B1_image.HiSide_OOBE\load	Скачивание	14822229	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	desktop.ini	Скачивание	386	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	usb.jpg	Скачивание	98942	192.168.88.13	178.170.168.19
30.10.2020 08:52:00	transceiver.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	136091	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	modem.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

На странице 1/100

Дополнительная информация

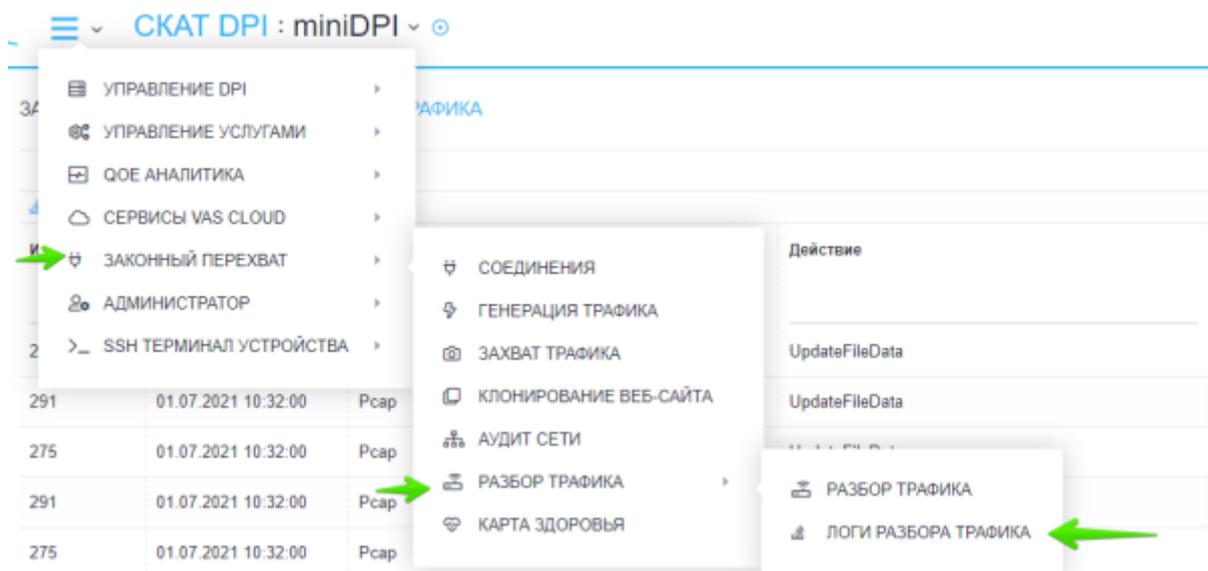
При нажатии на кнопку "Дополнительная информация"(?) откроется попап с дополнительной информацией о запросе:

- 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
		Ftp получателя	178.170.168.19
Дата	Файл	Eth	
		Тип Eth	0x00008000
		Eth отправителя	68:1d:ef:14:1d:d2
		Eth получателя	4c:5e:0c:f3:48:58
		Информация Ftp	
30.10.2020 08:52:00	stolka.jpg	Имя файла	tranceiver.jpg
30.10.2020 08:52:00	Рангола	Директория Ftp	/pub/Images/CON
30.10.2020 08:52:00	Link.jpg	Размер файла (байты)	127441
30.10.2020 08:52:00	DIR-310	Направление	Скачивание
30.10.2020 08:52:00	DIR-310	Файл	
30.10.2020 08:52:00	stolka.jpg	ИД файла	250
30.10.2020 08:52:00	usb.jpg	Файл ответа	wYCWwNgy0r:tranceiver.jpg
30.10.2020 08:52:00	tranceiver.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.

ЗАКОНЫЙ ПЕРЕХВАТ / ЛОГИ РАБОТЫ ТРАФИКА

Обновить список задач

Удалить задачу

Операция перехвата трафика

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 18:34:00	Резерв	ParseDecodedData	Вирт	Успешно		
275	01.07.2021 18:34:00	Резерв	ParseDecodedData	Mail	Успешно		
275	01.07.2021 18:34:00	Резерв	ParseDecodedData	Они	Успешно		
276	01.07.2021 18:34:00	Резерв	ParseDecodedData	Web	Успешно		
276	01.07.2021 18:34:00	Резерв	DecodeAction	Резерв	Успешно		
275	01.07.2021 18:34:00	Резерв	DecodeAction	Вирт	Успешно		
275	01.07.2021 18:34:00	Резерв	DecodeAction	Mail	Успешно		
275	01.07.2021 18:34:00	Резерв	DecodeAction	Они	Успешно		
276	01.07.2021 18:34:00	Вирт	DecodeAction	Mail	Успешно		

Просмотр информации о задаче

Постраничный переход

Количество записей на странице

180