

Содержание

- 1 Разбор трафика 3
 - Оборудование 3
 - Раздел 3
 - Задачи 4
 - Файлы 6
 - Результаты разбора 10
 - Логи разбора трафика 22

1 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:

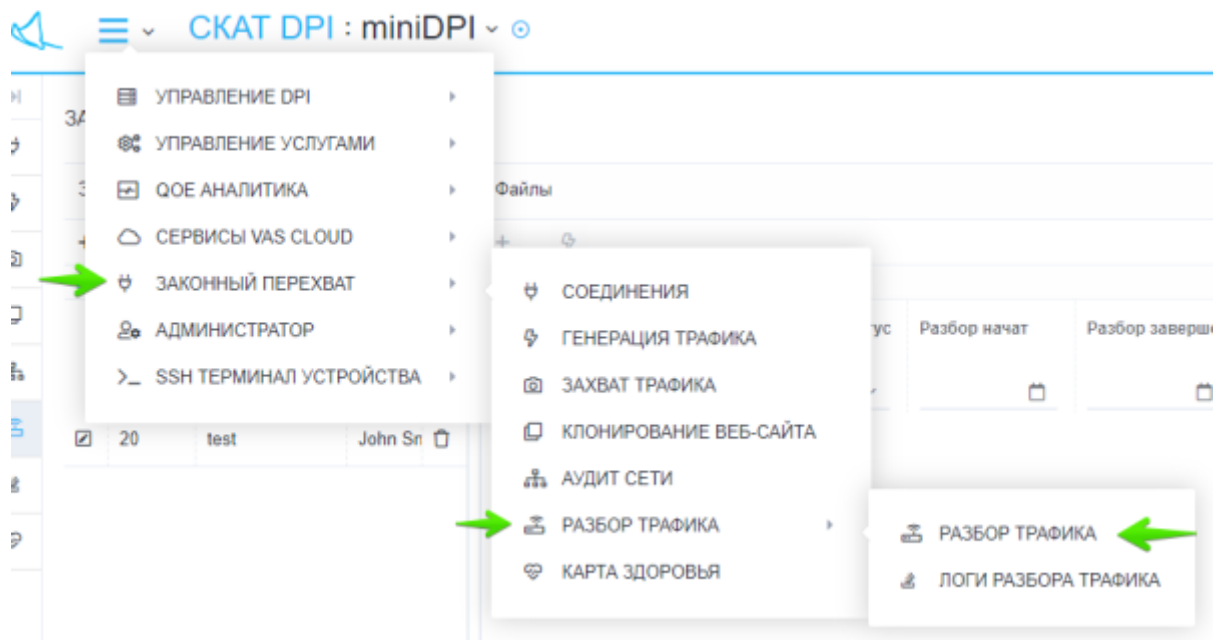
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

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.

Скриншот интерфейса SKAT DPI: miniDPI v2.20.0.5. Интерфейс разделен на две основные части: "Задачи" (слева) и "Результаты" (справа).

Левая часть (Задачи):

- Верхняя панель: "Законный перехват / Разбор трафика".
- Кнопка "+" для добавления задачи.
- Список задач с колонками: ID, Задача, Пользователь, Статус, Разбор начал, Разбор завершил.
- Действия над задачами: "Обновить список задач", "Добавить файл в задачу", "Перезапустить разбор трафика для файла", "Удалить задачу", "Редактировать задачу", "Скачать файл", "Удалить файл".

Правая часть (Результаты):

- Верхняя панель: "Обновить результаты разбора".
- Список результатов с колонками: Дата, Ура, Размер, Метод.
- Действия над результатами: "Обновить список файлов".

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.

Скриншот формы создания задачи "Разбор трафика".

Форму можно открыть, нажав на кнопку "+" в тулбаре над списком задач.

Форму создания задачи можно заполнить следующим образом:

- Название: Разбор трафика
- Описание: (пустое поле)

Кнопки: Отменить, Сохранить.

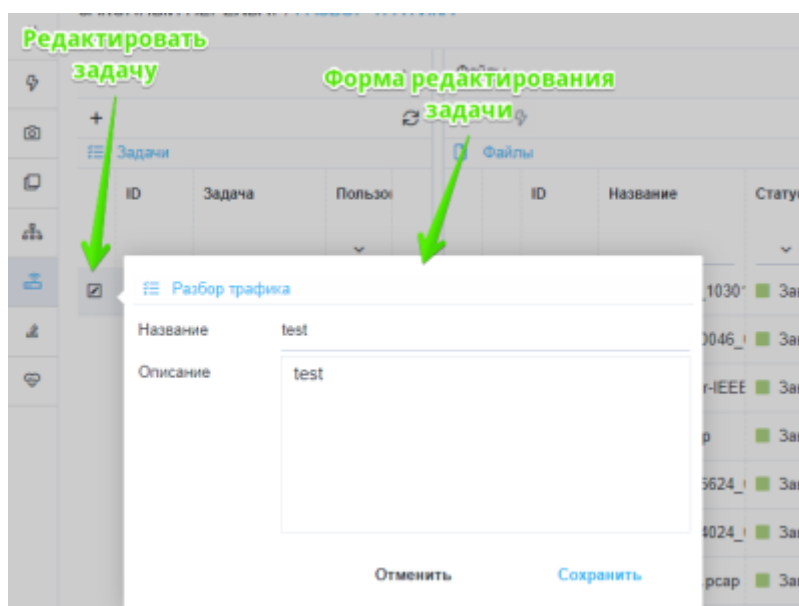
В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.



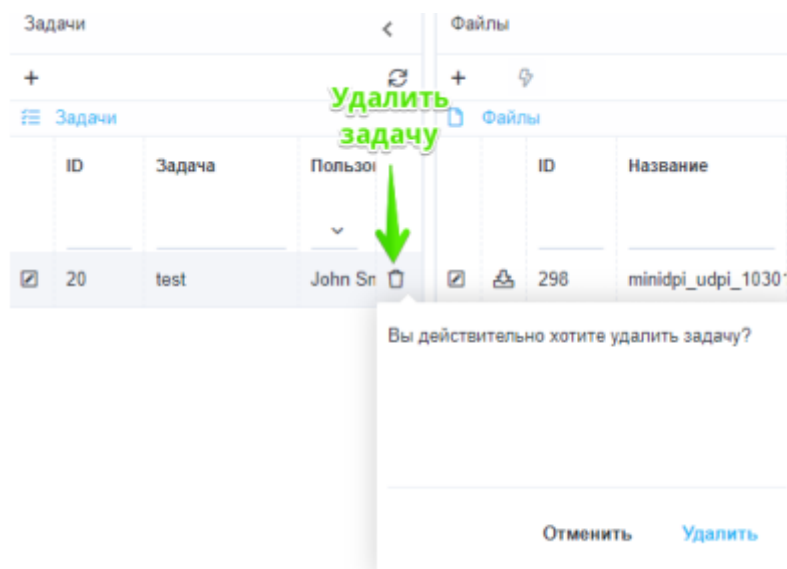
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

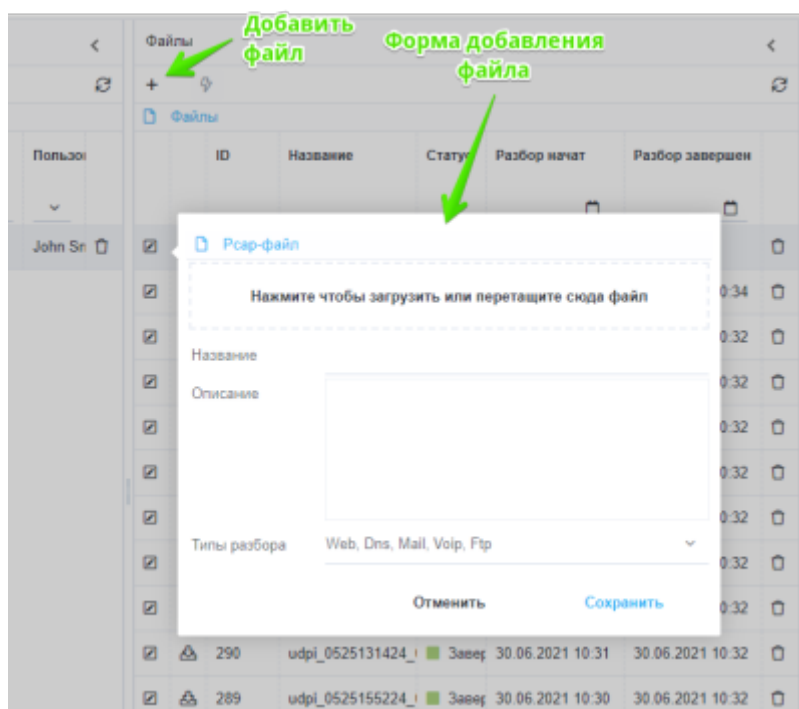


Файлы

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.



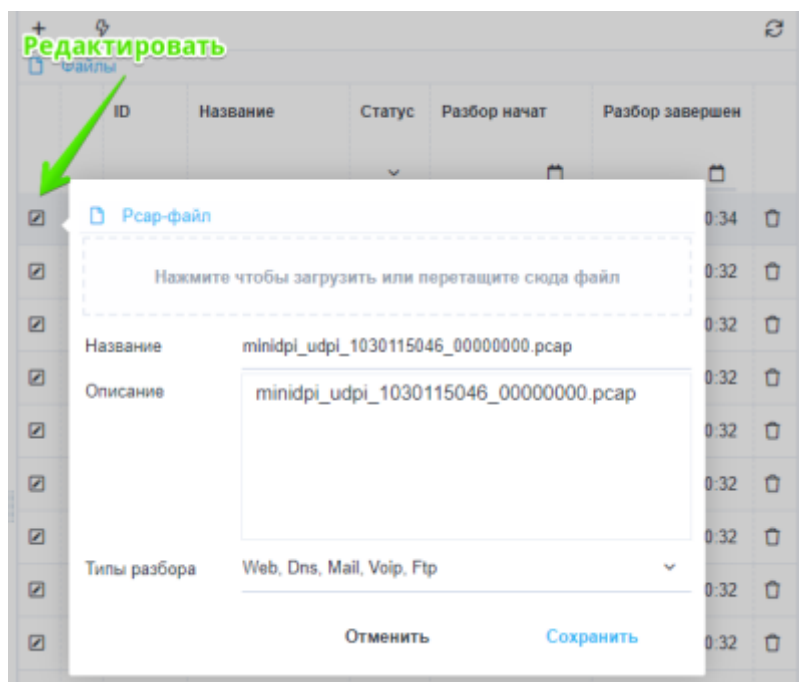
В открывшейся форме добавления файла:

- 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:

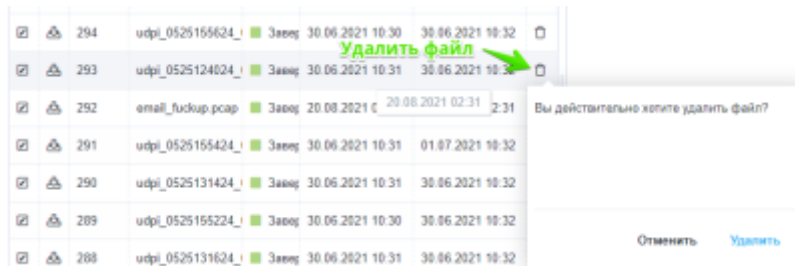
- Отображаемое название файла;
- Описание файла;
- Типы разбора трафика (Web,Dns,Mail,Voip,Ftp);

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

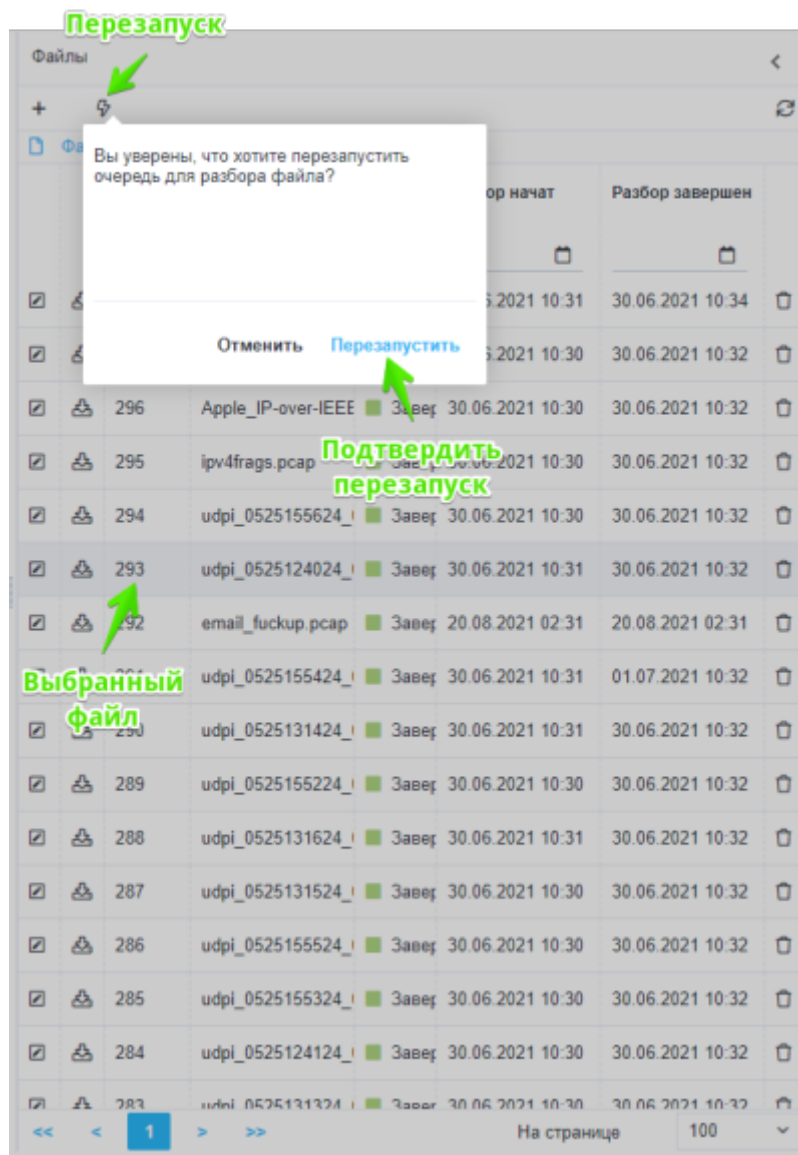
Для удаления файла нажмите на кнопку "Удалить" напротив существующего файла и подтвердите либо отмените действие.



Перезапуск разбора файла

Для перезапуска разбора файла:

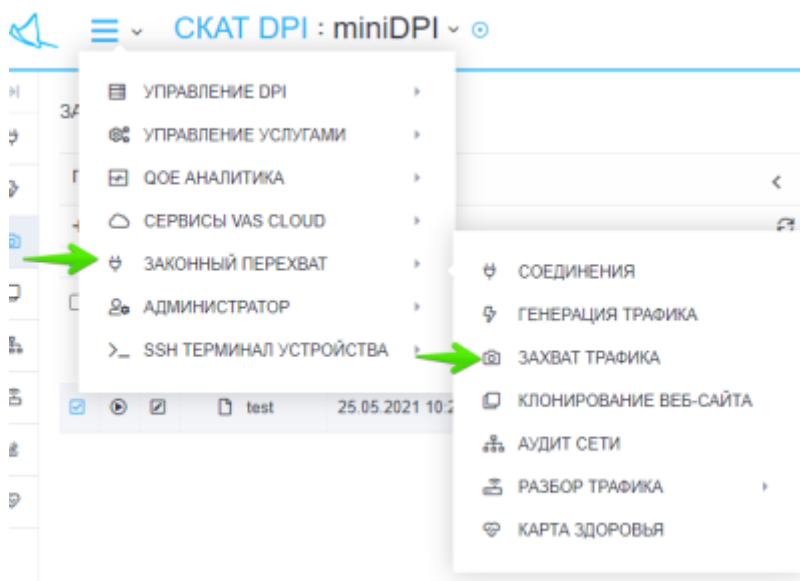
1. Выберите необходимый файл из списка;
2. Нажмите на кнопку перезапуска разбора в тулбаре;
3. Подтвердите либо отмените действие.



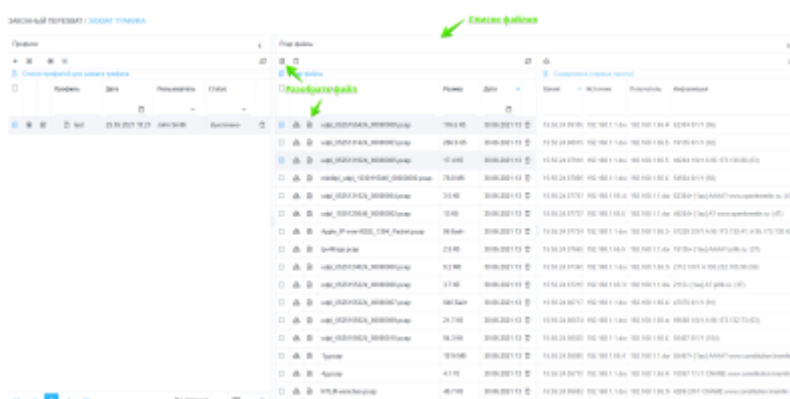
Импорт файлов из раздела захвата трафика

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.

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	ctdl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl cab?bf757d	0	GET	?
30.10.2020 08:53:00	ctdl.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	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/y9GgT364rvY.jpg	55126	GET	?

<< < 1 > >> 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 ТСП
- 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

Результаты

Web (45)

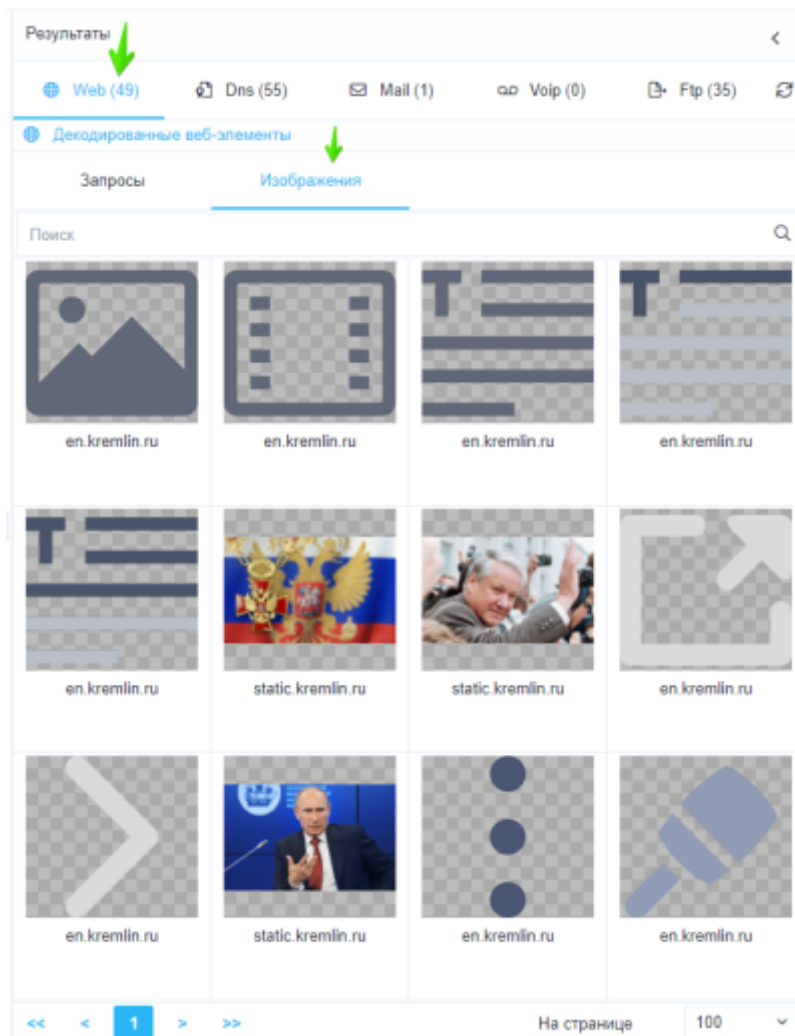
Декодированные веб-адреса

Запросы	IP	Порт получателя	Время Тср
Дата	Ури	Протокол Ip	6
30.10.2020 08:54:00	gscap	Версия Ip	4
30.10.2020 08:53:00	gtdk.u	Ip отправителя	192.168.88.13
30.10.2020 08:53:00	gtdk.u	Ip получателя	95.173.136.70
30.10.2020 08:52:00	oscap	Tcp Eth	0x00000000
30.10.2020 08:51:00	an.kre	Eth отправителя	68:1d:af:14:1d:d2
30.10.2020 08:51:00	an.kre	Eth получателя	4c:5e:0c:f3:4f:5b
30.10.2020 08:51:00	an.kre	Файл	290
30.10.2020 08:51:00	an.kre	Имя файла	minidpi_udp_1030115646_00000000.pcap
30.10.2020 08:51:00	an.kre	Файл ответа	2020
30.10.2020 08:51:00	an.kre		
30.10.2020 08:51:00	an.kremlin.ru/structure/president/standart		0 GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/structure-section/medium/Tsf5vnbldoIR47SJC5ORyStoIFBuKA		388095 GET
30.10.2020 08:51:00	static.kremlin.ru/media/events/presidents/medium/vjGqTJ6dnwY.jpg		55126 GET

На странице 100

Изображения

На 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)

Декодированные данные DNS

Дата	Хост	
30.10.2020 08:54:00	iecvlist.microsoft.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	ocsp.pki.goog	①
30.10.2020 08:54:00	pki-goog.l.google.com	①
30.10.2020 08:54:00	sb-esl.google.com	①
30.10.2020 08:54:00	pki-goog.l.google.com	①
30.10.2020 08:53:00	ctldl.windowsupdate.com	①
30.10.2020 08:53:00	ctldl.windowsupdate.com	①
30.10.2020 08:53:00	ctldl.windowsupdate.com	①
30.10.2020 08:53:00	DESKTOP-H465JAS.local	①
30.10.2020 08:52:00	windows.policies.live.net	①
30.10.2020 08:52:00	windows.policies.live.net	①

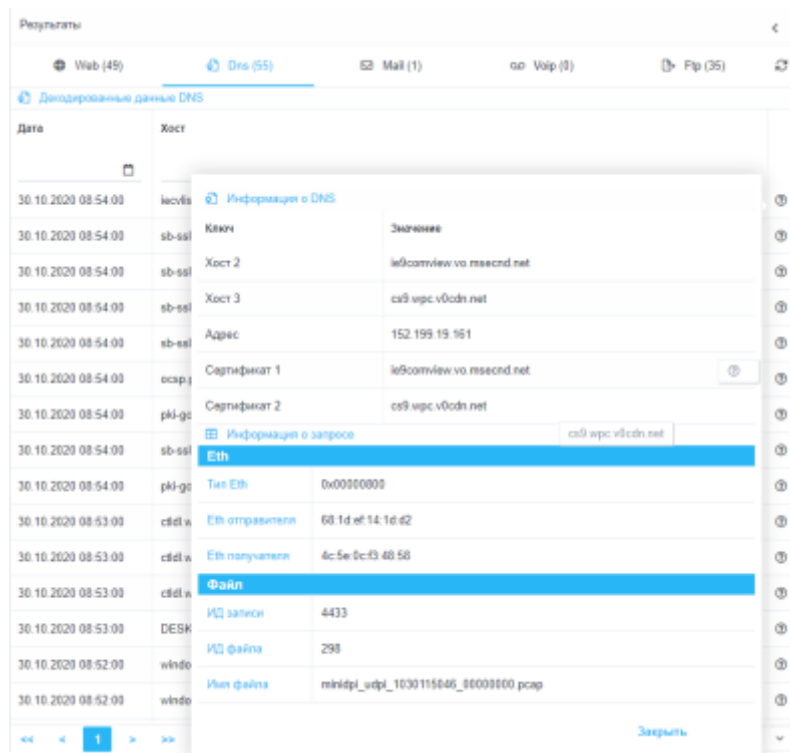
На странице 100

Дополнительная информация
о запросе

Дополнительная информация

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



Mail

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

В таблице доступны следующие данные:

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

Результаты

Web (45) Dns (0) Mail (4) Vpn (0) Ftp (0)

Детализированные данные Email

Дата	Отправитель	Получатель	Тема			
25.05.2021 07:51:00	VASE4 <vase4@vasemail.com>	VASE3 <vase3@vasemail.com>	Re: Subject Subject Subject Subj	Содержимое письма	📧	📎
25.05.2021 07:51:00	VASE4 <vase4@vasemail.com>	VASE3 <vase3@vasemail.com>	Subject Subject Subject Subject	Скачать ет-файл	📧	📎
25.05.2021 07:51:00	VASE3 <vase3@vasemail.com>	vase4@vasemail.com	Fwd: Fwd: Subject Subject Subject		📧	📎
25.05.2021 07:51:00	VASE3 <vase3@vasemail.com>	vase4@vasemail.com	Fwd: Fwd: Subject Subject Subject		📧	📎

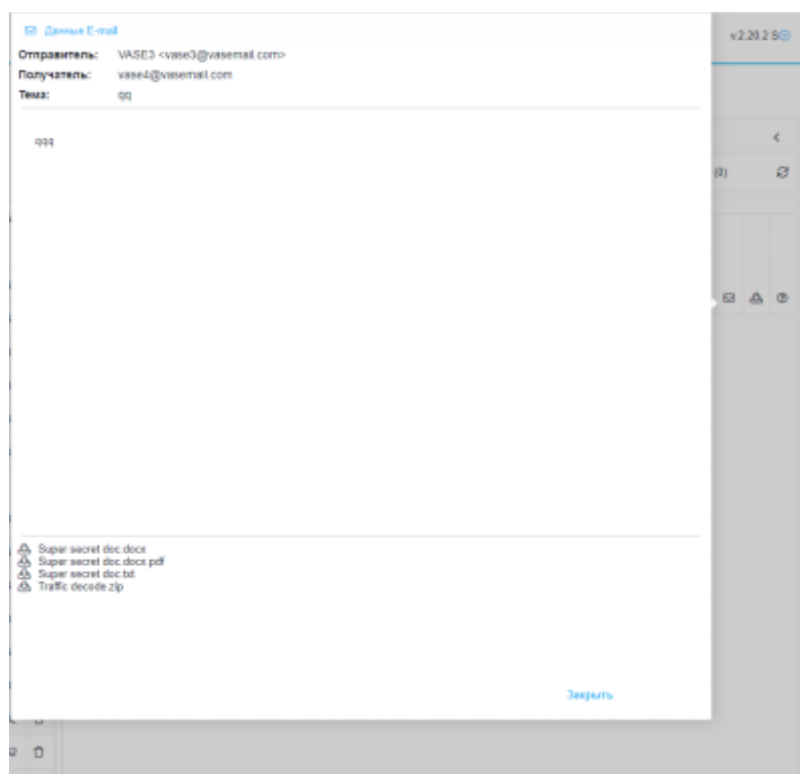
Дополнительная информация

На странице 100

Содержимое

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

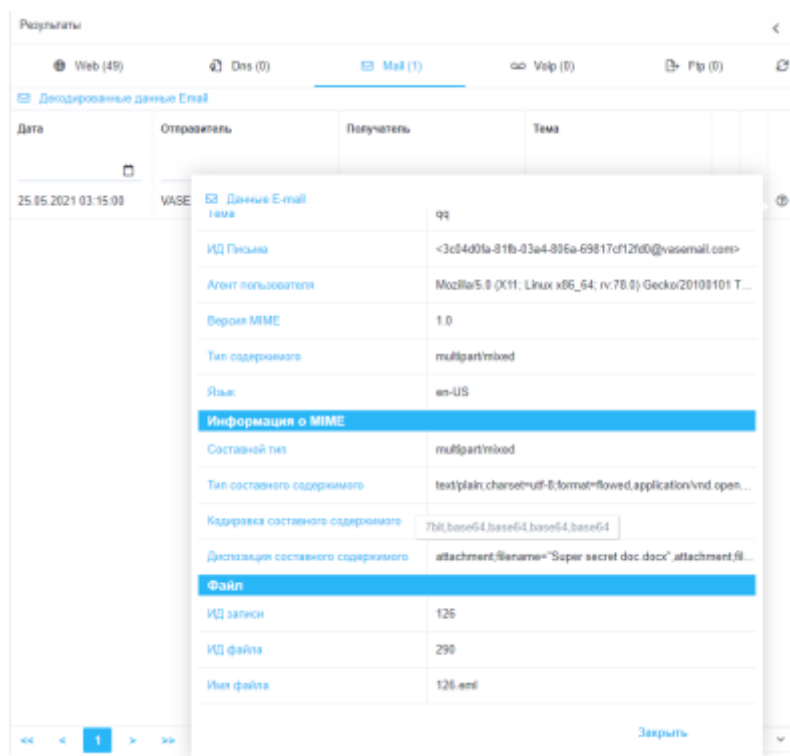
- Отправитель
- Получатель
- Тема письма
- Текст письма
- Список приложенных файлов к письму (можно скачать)



Дополнительная информация

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

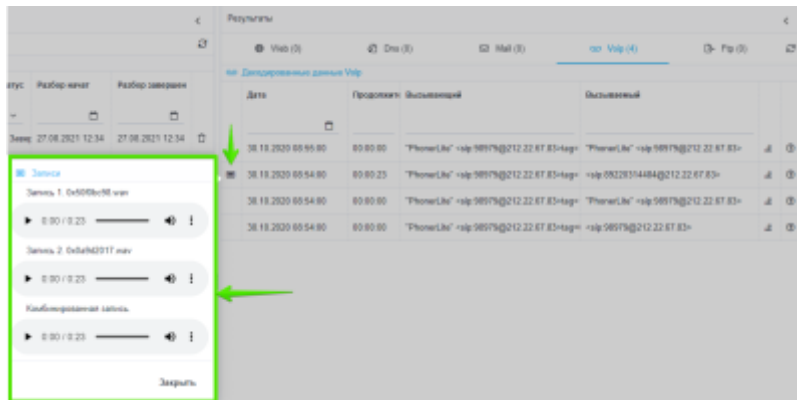
The screenshot shows a web application interface for Voip results. At the top, there are tabs for 'Web (8)', 'Dns (0)', 'Mail (0)', 'Voip (4)', and 'Ftp (0)'. The 'Voip (4)' tab is selected. Below the tabs, there is a table with the following columns: 'Дата', 'Продолжит', 'Вызывающий', and 'Вызываемый'. The table contains four rows of data. Green arrows point to specific elements: one to the 'Voip (4)' tab, one to the 'Дата' column header, one to the first row of data, one to the 'Вызываемый' column header, and one to the 'Вызываемый' column of the second row. There are also green text annotations: 'Доступна аудиозапись' (Available audio recording) pointing to the first row, 'Логи запросов' (Request logs) pointing to the 'Вызываемый' column header, and 'Дополнительная информация' (Additional information) pointing to the 'Вызываемый' column of the second row.

Дата	Продолжит	Вызывающий	Вызываемый
30.10.2020 08:55:00	00:00:00	"PhonerLite" <sip:56979@212.22.67.83>tag=	"PhonerLite" <sip:56979@212.22.67.83>
30.10.2020 08:54:00	00:00:23	"PhonerLite" <sip:56979@212.22.67.83>tag=	<sip:89220314404@212.22.67.83>
30.10.2020 08:54:00	00:00:00	"PhonerLite" <sip:56979@212.22.67.83>tag=	"PhonerLite" <sip:56979@212.22.67.83>
30.10.2020 08:54:00	00:00:00	"PhonerLite" <sip:56979@212.22.67.83>tag=	<sip:56979@212.22.67.83>

Аудиозапись

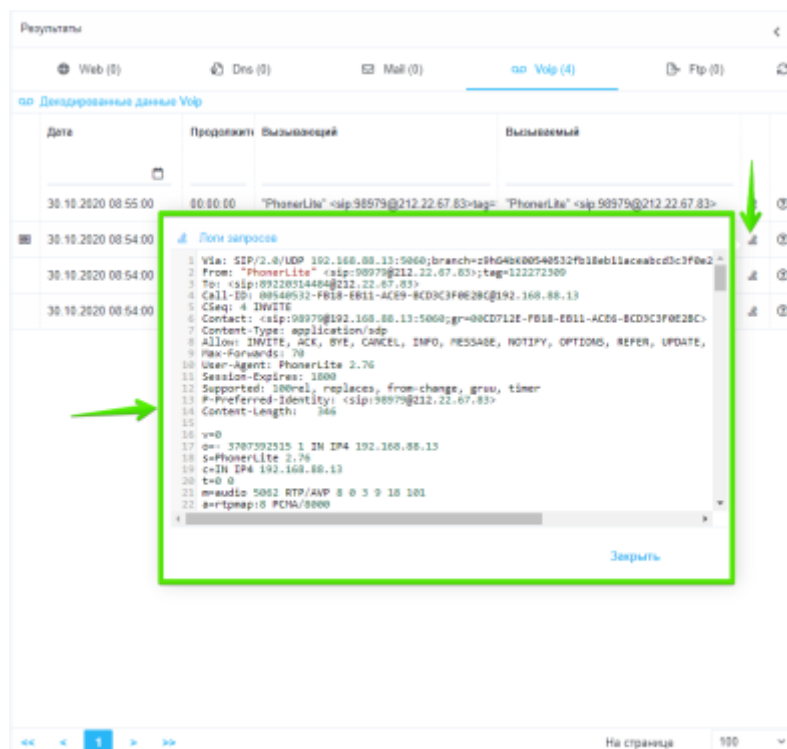
При нажатии на кнопку Записи откроется попап, в котором можно прослушать аудиозаписи:

- Вызывающего
- Вызываемого
- Комбинированную



Логи запросов

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



Дополнительная информация

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

- Порт отправителя
- Порт получателя
- Протокол IP
- 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
Заккрыть	

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) Voip (8) **Ftp (25)**

Декодированные данные Ftp

Дата	Файл	Направление	Размер	Клиент	Сервер	
30.10.2020 08:52:00	stolka_image.zip	Скачивание	5234345	192.168.88.13	178.170.168.19	🔗
30.10.2020 08:52:00	Pantone.tst	Скачивание	28	192.168.88.13	178.170.168.19	🔗
30.10.2020 08:52:00	elink_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\off	Скачивание	24693932	192.168.88.13	178.170.168.19	🔗
30.10.2020 08:52:00	DIR_300_B1_image.HiSide_OOBE\on	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	140707	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	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 100

Дополнительная информация

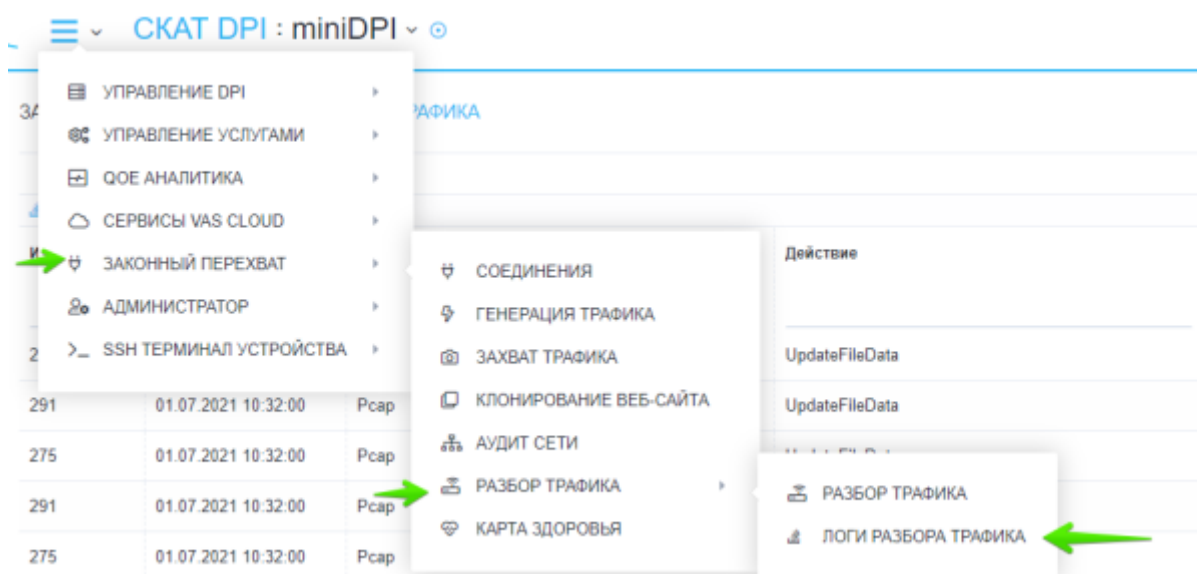
При нажатии на кнопку "Дополнительная информация" (?) откроется попап с дополнительной информацией о запросе:

- 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

Информация Ftp	
Версия Ftp	4
Ftp отправителя	192.168.88.13
Ftp получателя	178.170.168.19
Eth	
Тип Eth	0x0000800
Eth отправителя	68:1d:ef:14:1d:d2
Eth получателя	4c:5e:0c:f3:48:58
Информация Ftp	
Имя файла	tranciever.jpg
Директория Ftp	/pub/Images/ICON
Размер файла (байты)	127441
Направление	Скачивание
Файл	
ИД файла	250
Файл ответа	wYCWwNgy0r:tranciever.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.

[Обновить список задач](#)

Удалить

1

[Преглед информаци
о задаци](#)

Постраничный
переход

Количество записей на странице 100