

Table of Contents

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

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:

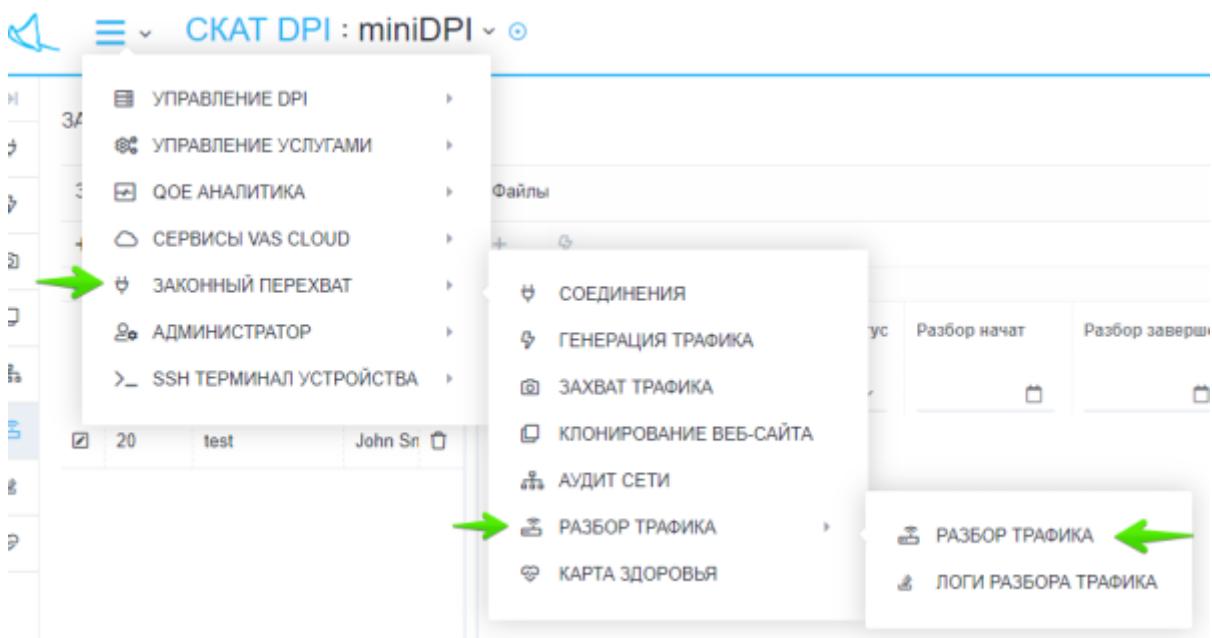
1. Процессор (CPU) 2.5 ГГц, 2 шт
2. Оперативная память (RAM) от 4 Гб
3. Жесткий диск (HDD) от 100 Гб
4. Операционная система Ubuntu 20.04

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 туллбаре над списком существующих задач.

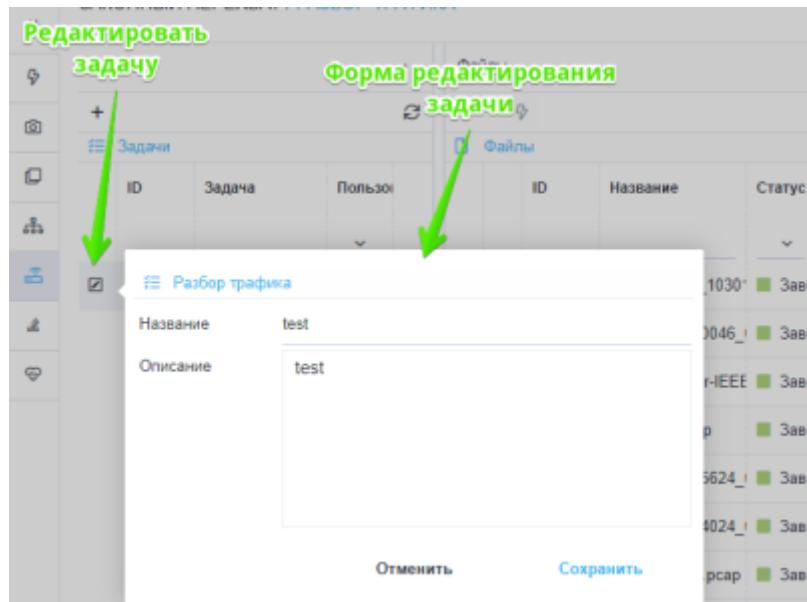
В открывшейся форме создания задачи введите:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Редактирование задачи

Для редактирования задачи нажмите на кнопку редактирования напротив существующей задачи.



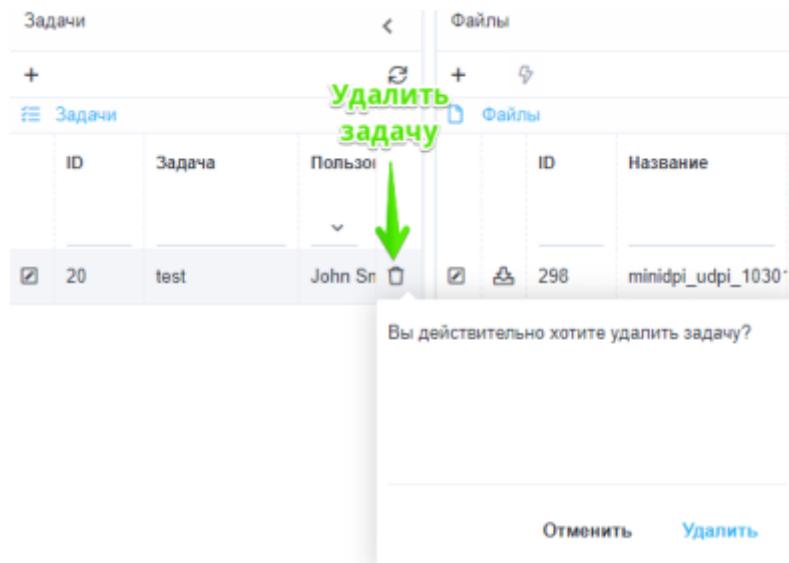
В открывшейся форме редактирования задачи измените:

- Название задачи
- Описание задачи

Нажмите кнопку "Сохранить".

Удаление задачи

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

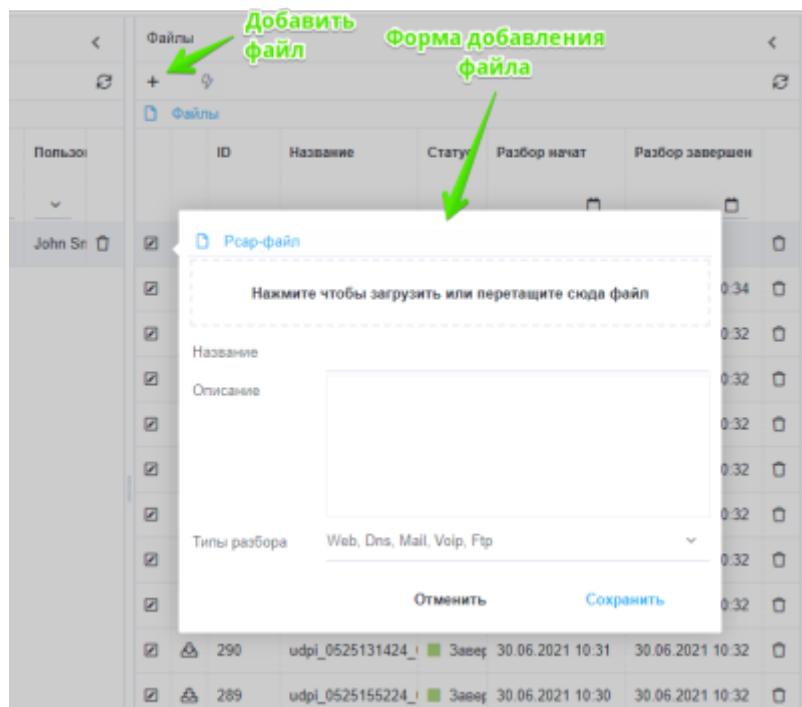


Файлы

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

Добавление файла

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



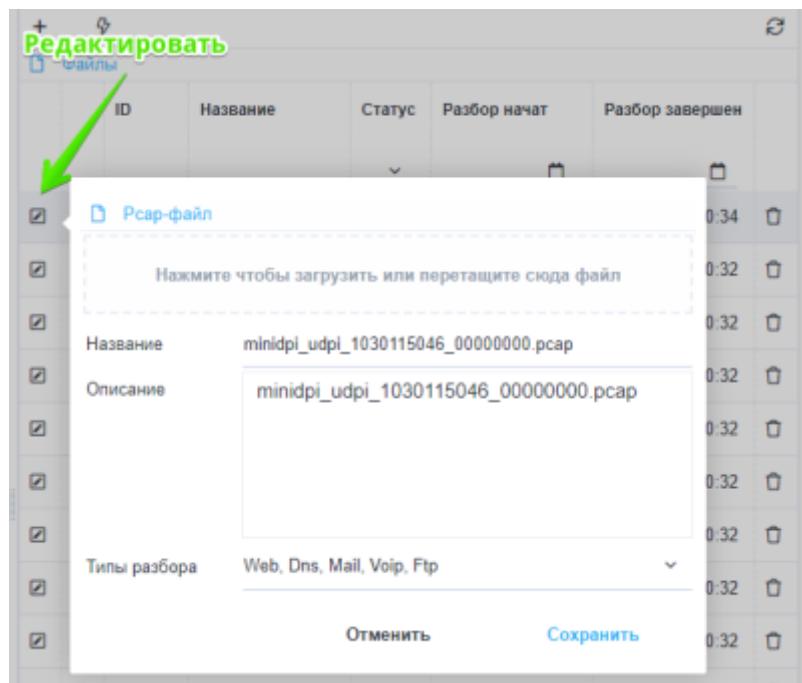
В открывшейся форме добавления файла:

- 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	2:31	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

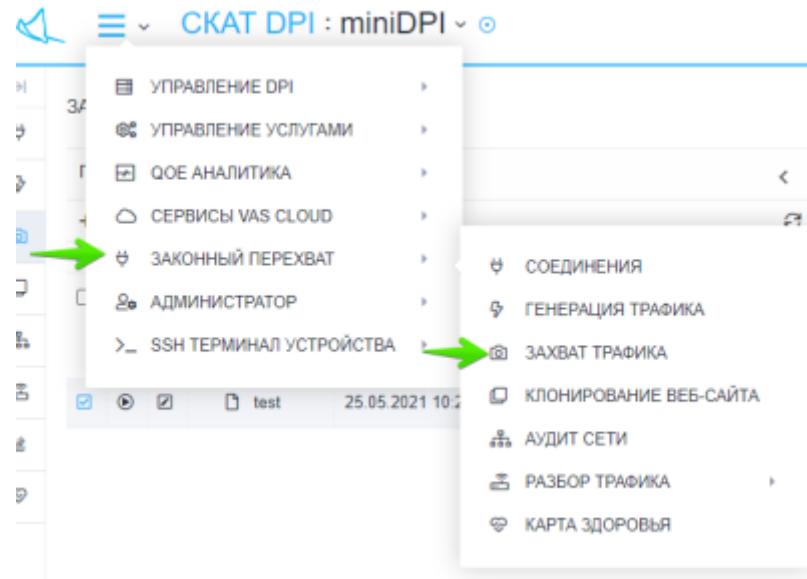
Файлы						
<input type="checkbox"/>				Время начал	Разбор завершен	<input type="button" value=""/>
<input checked="" type="checkbox"/>				30.06.2021 10:31	30.06.2021 10:34	<input type="button" value=""/>
<input checked="" type="checkbox"/>				30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	296	Apple_IP-over-IEEE	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	295	ipv4frags.pcap	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	294	udpi_0525155624_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	293	udpi_0525124024_	Завер.	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	292	email_fuckup.pcap	Завер.	20.08.2021 02:31	20.08.2021 02:31	<input type="button" value=""/>
Выбранный файл						
<input checked="" type="checkbox"/>	290	udpi_0525131424_	Завер.	30.06.2021 10:31	01.07.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	289	udpi_0525155224_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	288	udpi_0525131624_	Завер.	30.06.2021 10:31	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	287	udpi_0525131524_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	286	udpi_0525155524_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	285	udpi_0525155324_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	284	udpi_0525124124_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>
<input checked="" type="checkbox"/>	283	udpi_0525131324_	Завер.	30.06.2021 10:30	30.06.2021 10:32	<input type="button" value=""/>

100

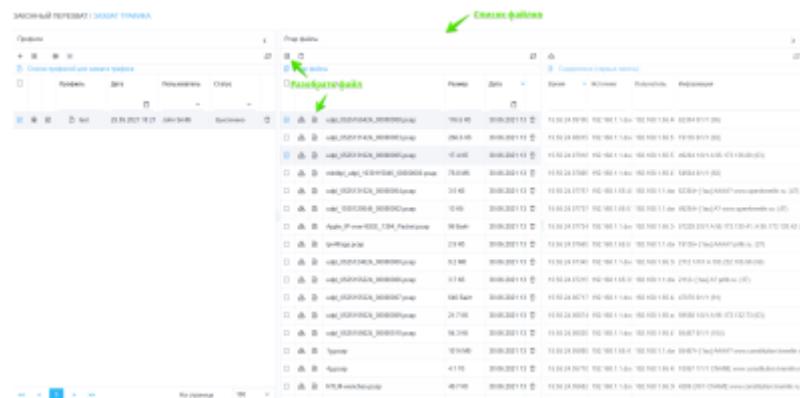
Импорт файлов из раздела захвата трафика

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.

ЗАКОННИЙ ПЕРЕХІД І РИЗИДОР ТРАНСІА

Задачі		Файли				
+	−	Файл	Файл	Файл	Файл	Файл
11 Задачі		Файли				
ID	Наймен.	Статус	Розподіл пакетів	Розподіл завантажен.		
28	test	John St				
296	minidp_adp1_1000_	Завантажено	30.06.2021 18:31	30.06.2021 18:34		
297	adp1_1000/1204842_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
298	266	Apple_iOS-over-EDGE_	Завантажено	30.06.2021 18:38	30.06.2021 18:32	
299	266	ipetkazip_rar	Завантажено	30.06.2021 18:38	30.06.2021 18:32	
294	adp1_05251954824_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
293	adp1_05251954824_	Завантажено	30.06.2021 18:31	30.06.2021 18:32		
292	email_Acknow_pptx	Завантажено	29.06.2021 02:31	29.06.2021 02:31		
294	adp1_05251954242_	Завантажено	30.06.2021 18:31	01.07.2021 18:32		
290	adp1_05251914242_	Результати розборки	30.06.2021 18:31	30.06.2021 18:32		
269	adp1_05251952242_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
268	adp1_05251916242_	Завантажено	30.06.2021 18:31	30.06.2021 18:32		
267	adp1_05251916242_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
268	adp1_05251953242_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
265	adp1_05251953242_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		
264	adp1_05251941242_	Завантажено	30.06.2021 18:38	30.06.2021 18:32		

Результати

Відмінні	Добре	Погано	Погано (2)	Погано (26)
Демонстрування від'ємного				
Записи		Підгруповані		
Дата	Час	Розмір	Метод	Очищення
30.10.2020	08:54:06	412	GET	
30.10.2020	08:53:01	0	GET	
30.10.2020	08:53:01	0	GET	
30.10.2020	08:52:01	279	GET	
30.10.2020	08:51:00	0	GET	
30.10.2020	08:51:00	269	GET	
30.10.2020	08:51:00	347	GET	
30.10.2020	08:51:00	219	GET	
30.10.2020	08:51:00	225	GET	
30.10.2020	08:51:00	224	GET	
30.10.2020	08:51:00	230	GET	
30.10.2020	08:51:00	0	GET	
30.10.2020	08:51:00	308816	GET	
30.10.2020	08:51:00	65526	GET	

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	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/	← Не кликабельный адрес	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	← Кликабельная ссылка	280	GET	?
30.10.2020 08:51:00	en.kremlin.ru/static/img/svg/video.svg	en.kremlin.ru/static/img/svg/photo.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	→ Дополнительная информация о запросе	131	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/Ty6y5wblsAqJR47S3O9Rju5bxIEBuKA	388035	GET	?	
30.10.2020 08:51:00	static.kremlin.ru/media/events/presidents/medium/y9GgT364rvY.jpg	55126	GET	?	

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 TCP
 - 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

Изображения

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

Результаты

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

Декодированные веб-элементы

Запросы Изображения

Помощь

Запрос	Изображение

На странице 100

DNS

На вкладке результатов разбора DNS отображаются хосты.

В таблице доступны следующие данные:

- Дата и время запроса
- Хост

Результаты	
Web (49)	Dns (55)
 Декодированные данные DNS	
Дата	Хост
30.10.2020 08:54:00	iecvlist.microsoft.com
30.10.2020 08:54:00	sb-sel.google.com
30.10.2020 08:54:00	oscar.rki.deeag
30.10.2020 08:54:00	pli-goog.google.com
30.10.2020 08:54:00	sb-sel.google.com
30.10.2020 08:54:00	pli-goog.google.com
30.10.2020 08:53:00	ctldl.windowsupdate.com
30.10.2020 08:53:00	ctldl.windowsupdate.com
30.10.2020 08:53:00	ctldl.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

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 запроса
- Идентификатор файла для разбора
- Имя файла для разбора

Результаты	
Web (49)	DNS (55)
Mail (1)	VoIP (0)
Декодированные данные DNS	
Дата	Хост
30.10.2020 08:54:00	iacvif
	Информация о DNS
30.10.2020 08:54:00	sb-ssl
	Ключ Значение
30.10.2020 08:54:00	sb-ssl
	Хост 2 iebcomview.v0.msecd.net
30.10.2020 08:54:00	sb-ssl
	Хост 3 сай wps.vcdn.net
30.10.2020 08:54:00	sb-ssl
	Адрес 152.199.19.161
30.10.2020 08:54:00	oscar
	Сертификат 1 iebcomview.v0.msecd.net
30.10.2020 08:54:00	pki-ge
	Сертификат 2 os9 wps.vcdn.net
30.10.2020 08:54:00	sb-ssl
	Информация о запросе
	Eth
30.10.2020 08:54:00	pki-ge
	Тип Eth 0x00000000
30.10.2020 08:53:00	ctd1w
	Eth отправителя 68:1d:ef:14:1d:e2
30.10.2020 08:53:00	ctd1w
	Eth получателя 4c:5e:0c:f3:48:58
30.10.2020 08:53:00	ctd1w
	Файл
30.10.2020 08:53:00	DEBK
	ИД записи 4433
30.10.2020 08:52:00	wind0
	ИД файла 298
30.10.2020 08:52:00	wind0
	Имя файла minidpl_wdpl_1030115046_00000000.pcap

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 (49) Dms (0) Mail (4) Voip (0) Ftp (0)

Декодированные данные Email

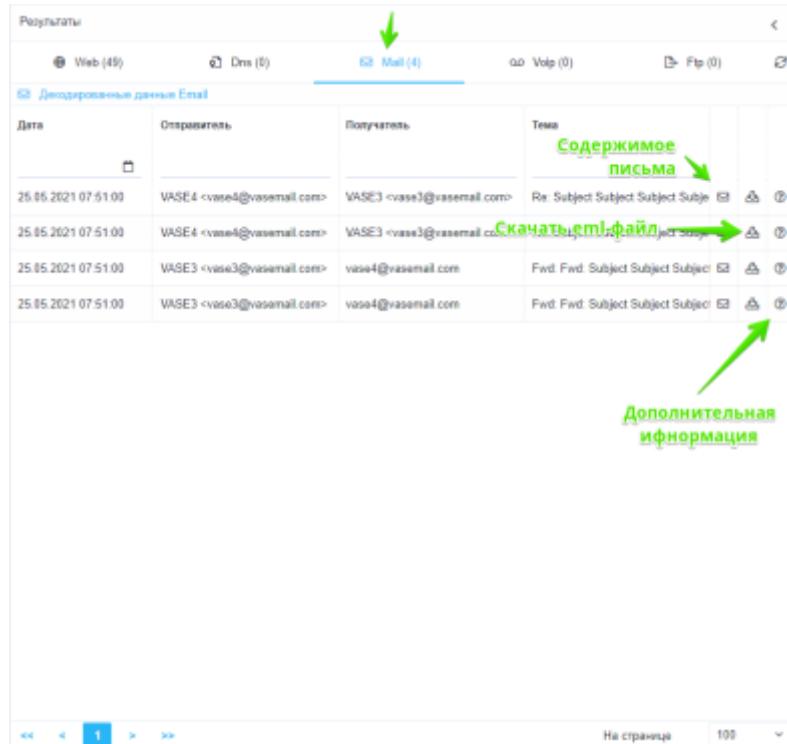
Дата	Отправитель	Получатель	Тема
25.05.2021 07:51:00	VASE4 <vase4@vasemail.com>	VASE3 <vase3@vasemail.com>	Re: Subject Subject Subject Subject
25.05.2021 07:51:00	VASE4 <vase4@vasemail.com>	VASE3 <vase3@vasemail.com>	Скачать email-файл
25.05.2021 07:51:00	VASE3 <vase3@vasemail.com>	vase4@vasemail.com	Fwd: Fwd: Subject Subject Subject
25.05.2021 07:51:00	VASE3 <vase3@vasemail.com>	vase4@vasemail.com	Fwd: Fwd: Subject Subject Subject

Содержимое письма

Скачать email-файл

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)

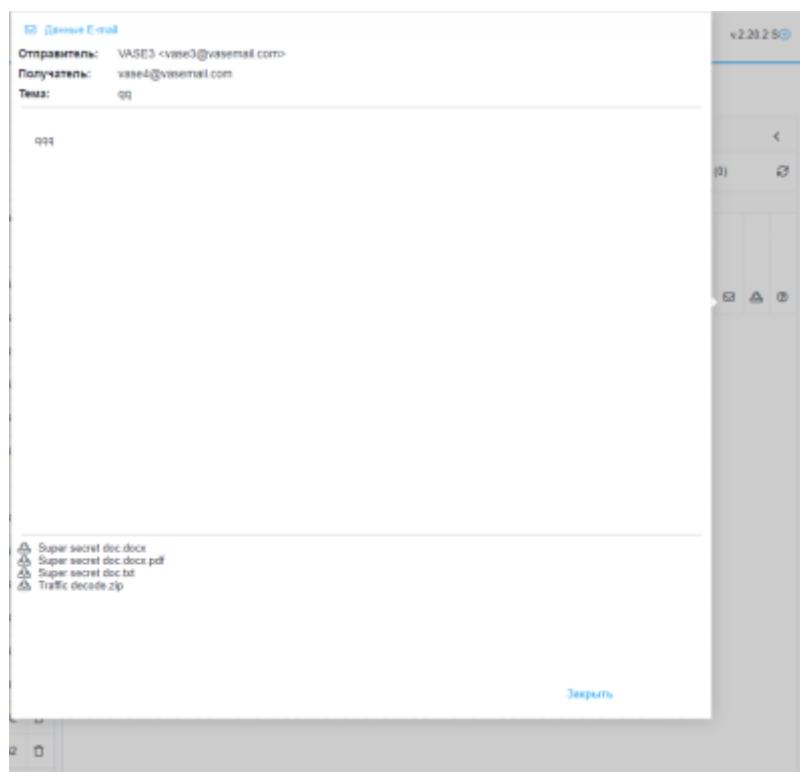
Данные Email

Отправитель: VASE3 <vase3@vasemail.com>
Получатель: vase4@vasemail.com
Тема: qq

qqq

Super secret doc.docx
Super secret doc.docx.pdf
Super secret doc.txt
Traffic decode.zip

Закрыть



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

Результаты

Web (49) DNS (0) Mail (1) VoIP (0) SIP (0) [Справка](#)

[Декодированные данные Email](#)

Дата	Отправитель	Получатель	Тема
25.05.2021 03:15:00	WASE		

[Данные E-mail](#)

Тема: [qq](#)

ИД Письма: <3c14d01a-81b-03e4-806a-69817cf12f60@wasemail.com>

Агент пользователя: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 T...

Версия MIME: 1.0

Тип содержимого: multipart/mixed

Язык: en-US

Информация о MIME

Составной тип	multipart/mixed
Тип составного содержимого	text/plain; charset=utf-8; format=flowed, application/vnd.open...
Кодировка составного содержимого	7bit,base64,base64,base64,base64
Диспозиция составного содержимого	attachment;filename="Super secret doc.docx";attachment;fil...

Файл

ИД записи	126
ИД файла	290
Имя файла	126.eml

« « < 1 > » » Закрыть

Voip

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

В таблице доступны следующие данные:

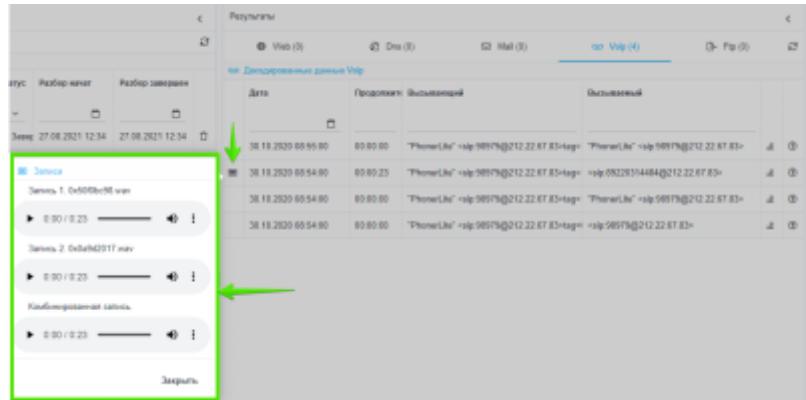
- Дата и время сессии
- Продолжительность сессии
- Вызывающий
- Вызываемый

Результаты				
Web (0)	Dns (0)	Mail (0)	Voip (4)	Ftp (0)
Декодированные данные Voip				
Логи запросов				
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>	

Аудиозапись

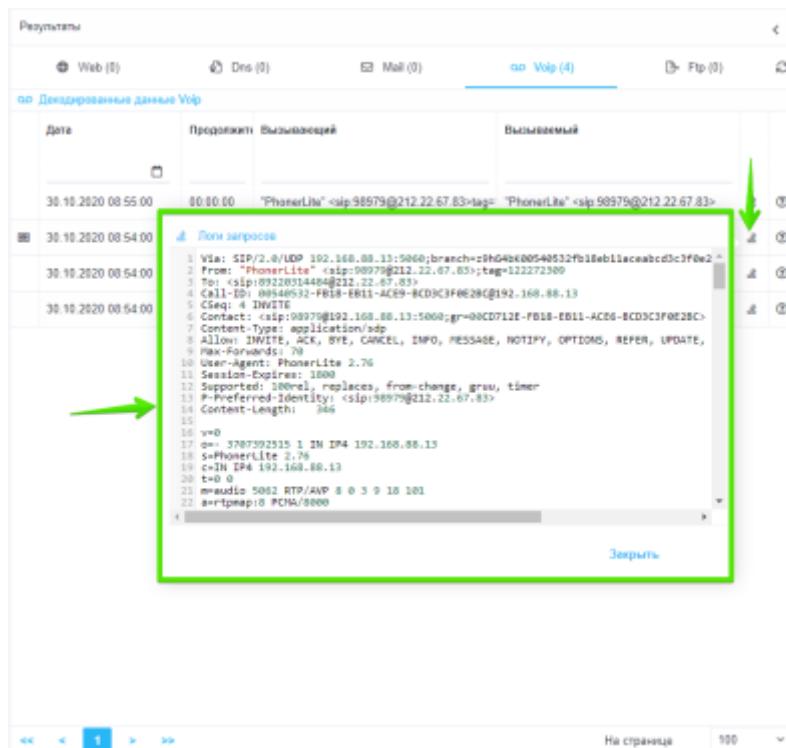
При нажатии на кнопку Записи откроется попап, в котором можно прослушать аудиозаписи:

- Вызывающего
- Вызываемого
- Комбинированную



Логи запросов

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

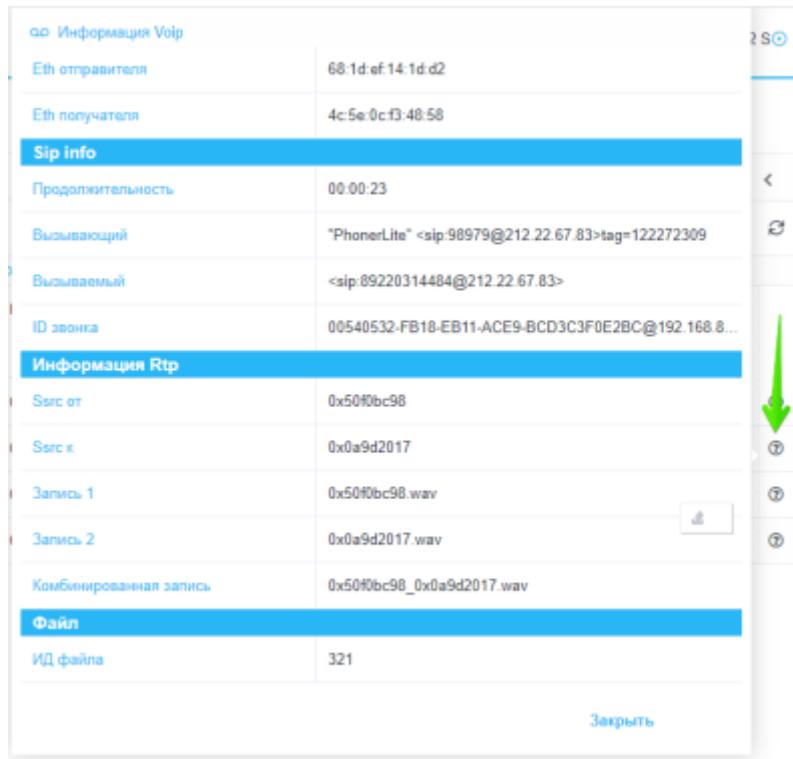


Дополнительная информация

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:0cf3:48:58
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	0xa9d2017
Запись 1	0x50f0bc98.wav
Запись 2	0xa9d2017.wav
Комбинированная запись	0x50f0bc98_0xa9d2017.wav
Файл	
ИД файла	321
Закрыть	

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) Dns (55) Mail (1) Voip (0) Ftp (36) 

Декодированные данные Ftp

Дата	Файл	Направление	Размер	Клиент	Сервер
30.10.2020 08:52:00	zloka_image.zip	Скачивание	5234345	192.168.88.13	178.170.168.19 
30.10.2020 08:52:00	Partest.txt	Скачивание	28	192.168.88.13	178.170.168.19 
30.10.2020 08:52:00	d-link_logo_image.zip	Скачивание	258678	192.168.88.13	178.170.168.19 
30.10.2020 08:52:00	DR-300_B1_Image.HiSide_COBE.tif	Скачивание	24693932	192.168.88.13	178.170.168.19 
30.10.2020 08:52:00	DR-300_B1_Image.HiSide_COBE.tif	Скачивание	14622229	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	sub.jpg	Скачивание	98542	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	postcard.jpg	Скачивание	145707	192.168.88.13	178.170.168.19 
30.10.2020 08:52:00	official.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	padem.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 

1 100

Дополнительная информация

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

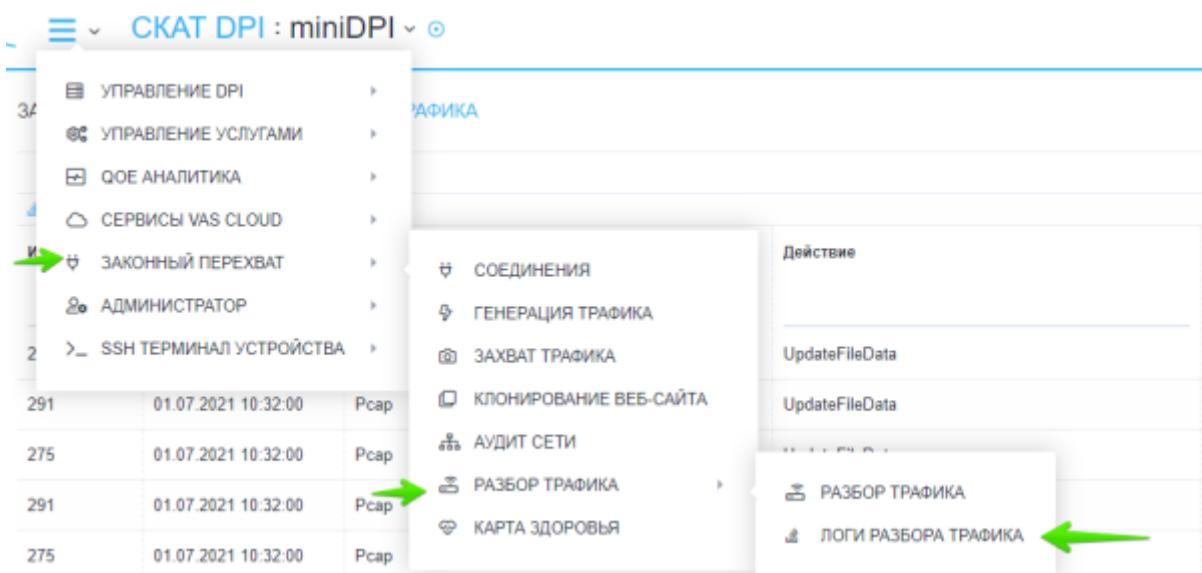
- Порт отправителя
- Порт получателя
- Протокол IP
- Версия IP
- IP отправителя
- IP получателя
- Тип Eth
- Eth отправителя
- Eth получателя
- Имя файла
- Директория Ftp
- Размер файла в байтах
- Направление
- Идентификатор файла для разбора
- Файл ответа

Результаты		Информация Ftp	
Web (49)		Eth	
Декодированные данные Ftp		Информация Ftp	
Дата	Файл	Имя файла	tranceiver.jpg
30.10.2020 08:52:00	stolka.jpg	Директория Ftp	/pub/Images/ICON
30.10.2020 08:52:00	Рамка...	Размер файла (байты)	127441
30.10.2020 08:52:00	alink.jpg	Назначение	Скачивание
30.10.2020 08:52:00	DIR-300	Файл	
30.10.2020 08:52:00	документ...	Ид. файла	298
30.10.2020 08:52:00	изв.jpg	Файл ответа	wYCWeNgy0r/tranceiver.jpg
30.10.2020 08:52:00	tranceiver		

[Закрыть](#)

Логи разбора трафика

Для перехода в раздел логов разбора трафика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Логи разбора трафика".



CKAT DPI : miniDPI

- УПРАВЛЕНИЕ DPI
- УПРАВЛЕНИЕ УСЛУГАМИ
- QOE АНАЛИТИКА
- СЕРВИСЫ VAS CLOUD
- ЗАКОННЫЙ ПЕРЕХВАТ**
- АДМИНИСТРАТОР
- SSH ТЕРМИНАЛ УСТРОЙСТВА

Ид	Время	Тип
291	01.07.2021 10:32:00	Pcap
275	01.07.2021 10:32:00	Pcap
291	01.07.2021 10:32:00	Pcap
275	01.07.2021 10:32:00	Pcap

РАЗБОР ТРАФИКА

- СОЕДИНЕНИЯ
- ГЕНЕРАЦИЯ ТРАФИКА
- ЗАХВАТ ТРАФИКА
- КЛОНРОВАНИЕ ВЕБ-САЙТА
- АУДИТ СЕТИ
- РАЗБОР ТРАФИКА**
- КАРТА ЗДОРОВЬЯ
- ЛОГИ РАЗБОРА ТРАФИКА**

Раздел Логов разбора трафика выглядит как на рисунке ниже.

