## Содержание

19 Законный перехват	3
Разбор трафика	3
Оборудование	3
Раздел	3
Логи разбора трафика	1

# 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 траффика в меню перейдите в раздел "Законный перехват"→"Разбор трафика"→"Разбора трафика".

$\triangleleft$			CKAT DP	l : minil	DPI	l ~ ⊙					
н 2 2	34	11 80 12	УПРАВЛЕНИЕ DPI УПРАВЛЕНИЕ УСЛУ QOE АНАЛИТИКА	ГАМИ	*	Фай	лы				
2 	-	0 # 20	СЕРВИСЫ VAS CLO ЗАКОННЫЙ ПЕРЕХЕ АДМИНИСТРАТОР SSH ТЕРМИНАЛ УС	UD ВАТ ТРОЙСТВА	*	+ 4	) ද බ	© СОЕДИНЕНИЯ ГЕНЕРАЦИЯ ТРАФИКА ЗАХВАТ ТРАФИКА	yc	Разбор начат	Разбор заверш
n 11		20	test	John Sn	Û			КЛОНИРОВАНИЕ ВЕБ-САЙТА АУДИТ СЕТИ РАЗБОР ТРАФИКА КАРТА ЗДОРОВЬЯ		2 РАЗБОР ТРАФ В ЛОГИ РАЗБОР	ИКА

Раздел Разбора трафика выглядит как на рисунке ниже.

~		~	CKAT DPI	: miniDPI	~ 0	0										JS John Smith ~	🗕 RU 🗸 🔬 🕚	۵ 🔍 ۵	v.2.	20.0 5
_	_										Обновит	ьсп	исок			$\sim$				
-11	3AK	онны	M REPEXENT / PA	SECP TPAPE	COK A	6			_		фай	лов	ł.							
¢				задам			A	оавить фаи	Ū.			_					Обновить ре			
9	3ag	39-04		<b>X</b>	97	1	83	adaay				•	Результаты				Concente pe	pastion		<
۵	+		Добавление	8	+	ç Oair		Перезапус разбор тра	тить фика			3	Web (49)		🖏 Des (55)	63 Mail (1)	QLD Valp (0)	D Fi	(35)	3
		10	задачи	Born on	-		in.	для файла	Came	Danfan unur	Barfon same		<ul> <li>Декодированные веб-</li> </ul>	anewerin	ы					
4		10		1011200			10	01:310040.2	charge	Peppop Harian	Patoop savepare		Запросы		Изображения					
m				~					~	0	0		B	Mar.						
æ	2	20	test	John Sr 📋	2	۵	298	minidpi_udpi_1030	anos	30.06.2021 10:31	30.06.2021 10:34	Û	Maria	shu				Paswag	merog	
4	k				12	Δ.	297	udpi_1030120046	B Gener	30.06.2021 10.30	30.06.2021 10:32	0	0						~	
ę					12	Δ.	295	Annia IR-over-IEEE	- Samer	38.06.2021.10.30	30.06.2021.10.32	0	30.10.2020 08:54:00	ocsp.pki	appaiats1o1core			472	GET	Ø
		١.		Удалит	b.,	~	204	had been seen		35.05.3031.10.30	20.06.2021.10.22	•	30 30.10.2020 08.53.00	ctid wine	dovisupdate.com/msdownlo	ad/update/v3/static/truste	drien/disallowedcertatl.cab	1 <del>6757d</del> 0	GET	Ø
Pe	Редактировать з задачу		овать	задачу	( <sup>6</sup>		293	dovenage bosh	- Japes	34.04.2021 10.30	30.00.2021 10.32		30.10.2020 08:53:00	ctid wine	dovsupdate.com/mediovnio	ad/update/c3/static/huste	dr/en/disallowedcertstl.cab	261fc1 0	GET	Ø
				2		294	udpi_0525155624_	3eeet	30.06.2021 10:30	10:30 30.06.2021 10:32 10:31 30.06.2021 10:32	Û	20.40.2020.00.02.02		tial windowaypdate.com/madownioad/updater/Jotatic/husted/en/disallowed/setail.cat/261 csp.digloert.com/		270				
					2	⇔	293	udpi_0525124024_	B Beeer	30.06.2021 10:31	30.06.2021 10:32	0	30.10.2020 00.52.00	ocsprag	(Cert.Com/			2/9	GET	w
					8	۵	292	email_fuckup.pcap	B Seens	38.06.2021 10.30	30.06.2021 10:32	0	30.10.2020 08:51:00	on kremi	iin.ru/events/president/news	k		0	GET	œ
					2	۵	291	udol 0525155424	and Same	38.05.2021.10.31	01.07.2021 10:5 01	07.203	21 10:32	en kremi	in ruʻstaticimpisypiphota sr	19		260	GET	œ
					-								30.10.2020 08:51:00	en kremi	in rahtaticimpiavpivideo.av	19		347	GET	®
					12	23	291	uopi_0525131424_	ases	30.06.2021 10:31	30.06.2021 10:32	0	30.10.2020 00:51:00	en kremi	in.ru/static/img/svg/big_text	Lavg		210	GET	0
					2		289	udpi_0525155224_	B 3eeet	30.06.2021 10 XA	алиты 12	0	30 10 2020 00 51 00	on kunni	in additional and a second second	ent aux		226	GET	
					2	⇔	288	udpi_0525131624_	📕 Завер	30.06.2021 10.31	36 06 2021 10:32	٥	50.10.2020 00.51.00	OIL SUGAR	NUT SHALL HIS STORE A	00.010		66.9	OE1	w
			Редактиро	вать	2	۵	287	udpl_0525131524_	anes	30.05.2021 10:30	30.06.2021 10:32	0	30.10.2020 08:51:00	en kremi	in ru/static/imp/svpimedium	_boxt.svg		224	GET	œ
				файл	12	۵	205	udol 0525155524	Janes	30 05 2021 10:30	30.05.2021.10:32	0	30.10.2020 08:51:00	en kremi	lin.na/eventa/president/news	vicalandari2020		231	GET	®
			Скачать ф	aŭn —									30.10.2020 08:51:00	en kremi	lin.ru/structure/president/sta	indart		0	GET	œ
			ann sann de		1	-63	285	udpi_0525156324_	a seet	30.06.2021 10:30	30.06.2021 10:32	U	30.10.2020 08:51:00	static, kre	enlin.ru/media/events/struct	ture-section/medium/Tv6v	SubisAq.R475309Riu6bul	EBUKA 388035	GET	0
					Ø	≙	284	udpl_0525124124_	3aeet	30.06.2021 10:30	30.06.2021 10:32	Û	30 10 2020 08 51 00	static ins	amlie nu/madia/avaets/wasik	donts impetient i 40 mil 40 mil 46	wVine	55126	OFT	(B)
				400	121	۸	281		- 3aaar	38.06.2021 10:50	30.06.2021.10-32	•	39.10.2020 00.21.00	1000.00			ILL IV I	20120	400	w.
	**		На странице	100 9	**	*	1	3 33		На страни	4e 100	Ψ.	<c 1="" <=""></c>	35			н	а странице	100	~

#### 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.

ЗАК	ОННЫЙ ПЕРЕХВ	АТ / РАЗБОР ТРАФИК	Ą		
За,	дачи Доб	авить задачу	Фай	лы	
+	Z	B	+	9	
£≣	Задачи 🔍	орма создания	0	Файлы	
	ID Задача	задачио		ID	Название
	f⊟ Разбор траф	бика			
	Название				
	Описание				
		Отменит	5	Co	хранить

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.

зада	чу		Форма реда	ктирован	ия							
+			<i>а</i> задачи									
£E 3	Бадачи		9	Файлы								
	ID 3	адача	Пользон	ID	Название		Статус					
1												
	⊞ Разбо	р трафика				10301	<b>3</b> ar					
	Название	test				0046_0	<b>3</b> as					
	Описание	te	st			r-IEEE	🔳 Зав					
						p	🔳 Зав					
						5624_0	📕 Зан					
						4024_0	📕 3ar					
			Отменить	Co	хранить	pcap	a 3ar					

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.

<	Φai	inu da	обавить айл	Форма до	бавления йла		<
ខ	+	9			/		e
	D	Файлы			/		
Пользон		ID	Название	Статуу	Разбор начат	Разбор завершен	•
~		_			m	0	
John Sn 📋		D Pcap-d	райл				Û
	Ø	Ha	жмите чтобы	ы загрузить или п	еретащите сюда ф	айл 0:34	Û
		Название				0:32	O
	Ø	Описание				0:32	Û
	Ø					0:32	٥
						0.32	Û
	Ø	Turni nasta	wa Wab	Dos Mail Voin Etr		0:32	Û
		типы разоо	ipa meu	, una, man, voip, rig	r	0.32	Û
	Ø			Отменить	Сохр	анить 0:32	Û
		A 290	udpi_0525	131424_( 📕 Завер	30.06.2021 10:31	30.06.2021 10:32	0
		A 289	udpi_0525	155224_( 🔳 Завер	30.06.2021 10:30	30.06.2021 10:32	Û

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.

Ред	актировать							3				
	ID Has	вание	Статус	Разбор нача	т Ра	збор зав	ершен					
			~		m							
	🗅 Рсар-файл						0:34	Û				
	Нажмите	э чтобы загруз	ить или п	еретащите с	ода файл		0:32	Û				
	Название	minidpi udpi	minidpi udpi 1030115046 0000000.pcap									
	Описание	minidpi_u	minidpi udpi 1030115046 0000000.pcap									
Ø							0:32	Û				
	*	Web Dee M	all Main El	-			0:32	Û				
	типы разбора	vveb, Dhs, Ma	Ý	0:32	Û							
			Отменить		Сохранит	пь	0:32	Û				

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.

Ø	۵	294	udpl_0525155624_1 3aeeg 30.06.2021 10.30 30.06.2021 10.32	0
Ø	۵	293	udpi_0525124024_1 - 3amer 30.06.2021 10.31 30.06.2021 10.3	0
2	۵	292	email_fuckup.pcap = 3apeg 20.08.2021 0 20.08.2021 02:31 2:31	Вы дейстентельно хотите удалить файл?
Ø	۵	291	udpi_0525165424_1 📕 3æeg 30.06.2021 10:31 01.07.2021 10:32	
Ø	۵	290	udpi_0525131424_! 📕 Завер 30.06.2021 10.31 30.06.2021 10.32	
2	۵	289	udpi_0525155224_i aapeg 30.06.2021 10:30 30.06.2021 10:32	0 m N
Ø	۵	288	udpi_0525131624_1 📕 Завед 30.06.2021 10:31 30.06.2021 10:32	Отменить 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											
Φai	йлы	1				<					
+		\$				ø					
٥	Фа	Вы уверены	, что хотите перезапустить								
		очередь для	а разбора файла?	ор начат	Разбор завершен						
	6			5.2021 10:31	30.06.2021 10:34	Û					
	6		Отменить Перезапустить	5.2021 10:30	30.06.2021 10:32	Û					
	₼	296	Apple_IP-over-IEEE Steer 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	盎	295	ipv4frags.pcap	CK	30.06.2021 10:32	Û					
	♣	294	udpi_0525155624_( 🔳 Завер 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	ى	293	udpi_0525124024_( 📓 Завер 3	0.06.2021 10:31	30.06.2021 10:32	Û					
	ا	.92	email_fuckup.pcap 📕 Завер 2	0.08.2021 02:31	20.08.2021 02:31	Û					
Вы	бр	ан̂н́ый	udpi_0525155424_( 📕 Завер 3	0.06.2021 10:31	01.07.2021 10:32	Û					
	썦	айд,	udpi_0525131424_( 📕 Завер 3	0.06.2021 10:31	30.06.2021 10:32	Û					
	₼	289	udpi_0525155224_( 📕 Завер 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	₽	288	udpi_0525131624_( 📕 Завер 3	0.06.2021 10:31	30.06.2021 10:32	Û					
	ى	287	udpi_0525131524_( 📕 Завер 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	&	286	udpi_0525155524_( 🔳 3aseg 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	ا	285	udpi_0525155324_( 📕 3ase; 3	0.06.2021 10:30	30.06.2021 10:32	Û					
	₼	284	udpi_0525124124_( 📕 Завер 3	0.06.2021 10:30	30.06.2021 10:32	Û					
2	A	วดว	urdni 0525131324 i 🔲 3aoar 3 > >>	о об 2021 10-30 На стран	30.06.2021.10-32 ице 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.

-								in.		-		_							
									. a										
	-	-	rol yrs sans						κ.	-					a comme	in jungen a same	servel		
		1	oden.	341	Processory of	CHEM		D	uù	2	negala.	PL/HD	201		Tpost 1	B(100ml	francisco de	Reparement	
			b wi	000000	10120	Becceso.	e		A. 1	c	41.001043.00000.au	101.0	20.2		111111	10100.14	10.101.014	101041011100	
									4.1	2	00.057743.00890.009	2913-15			111110-001	10.00.14		10105-0111-003	
									4.1	a	application and and apply the	10.000	10.00		101020-0010	101001-001		NUMBER OF STREET, STRE	
									4.1	a	and the second s	24.008	20.00	0.00	101020-0108	-		And a low (ki)	
										8	and ADVINCE, NUMBER OF	2140	20.0	0.0.0	101024-071	-	100.000.004	EDD- (Inc)AMP-recognitionity	
									a. 1	8	00,00000,0000,000	12.49	20.2	0.0 0	11012121	10.00100.0	10.1011.04	RDD (m)/Consequencies ()	
									a. 1		Aph. Prov 522, 224, Notice on	10 East	20.2		10000	10.00114	10.10110.0	DEDUCTION CONTRACTOR	
									a. 1		policy page	11.0	20.2	1 I I I	111111-0111-01	10.001000	10.1011.00	TERM DECAMPUSED IN	
									4.1	2	0.00106.0000.00	12.00	10.00		1110.000	101003-04	100,000,000	1412 1414 14106 1212 1412 1412 1412	
									4.1	a.	46,0527523,00000,049	1116	10.00	111 2	101024-0024	101001003		2013-(3m)Af pRess (07)	
									4.1	a	and Alexandra Alexandra	101547	20.00	10.9	101024-0070	100100-014		allele ann per	
								п	4.1	8	and Alexandra Statistics	28.798	20.0	0.00	101024-007	101003-044		NUM 1013-01-0213(02)	
								п		8	weight the part of	16.210	20.2	0.0.0	10.0024.0000	10.00114	100.000.000.0	1007-017 (100	
									a. 1		Type or a local sector of the local sector of	101100	20.2	0.0 0	10.00.00.000	10.10110-0	10.1011.04	10405 (ImpANN' recommission)	
											Autore Contraction	4110	20.2		111124-001	10.00114	10.10110.0	1047 IV1 DMB was smallabout	

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).

Ø	D D		
			×
	Задача	Новая задача	~
Û	Имя задачи		
	Типы разбора	Web, Dns, Mail, Voip, Ftp	~
		Отменить Примен	ИТЬ

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

### Результаты разбора

В разработке.

Ftp

В разработке.

## Логи разбора трафика

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

_ <b>=</b> ~	CKAT DPI : mini	DPI	× 0						
34 SC YTTF	<ul> <li>УПРАВЛЕНИЕ DPI</li> <li>УПРАВЛЕНИЕ УСЛУГАМИ</li> <li>ООБ АНАЛИТИКА</li> </ul>		λφηκα						
	CEPBUCH VAS CLOUD		8 0050HUE1HU	Действие					
<ul> <li>2 &gt;_ SSH ТЕРМИНАЛ УСТРОЙСТВА</li> </ul>		•	<ul> <li>СОЕДИНЕНИЯ</li> <li>ГЕНЕРАЦИЯ ТРАФИКА</li> <li>ЗАХВАТ ТРАФИКА</li> </ul>	UpdateFileData					
291	01.07.2021 10:32:00	Рсар	КЛОНИРОВАНИЕ ВЕБ-САЙТА • АУЛИТ СЕТИ	UpdateFileData					
275	01.07.2021 10:32:00	Pcap Pcap	<ul> <li>В РАЗБОР ТРАФИКА</li> <li>В РАЗБОР ТРАФИКА</li> </ul>	😤 РАЗБОР ТРАФИКА					
275	01.07.2021 10:32:00	Pcap	🐵 КАРТА ЗДОРОВЬЯ	🔬 ЛОГИ РАЗБОРА ТРАФИКА					

Раздел Логов разбора трафика выглядит как на рисунке ниже.

монныйт	NEPEXBAT / JODA PAS	GOPA TRADUKA	Обновить список				
d Dungman p	partispa rpadana						Удали
(E) C Special	aru G	Test	Aprile these	Ten paulopa	Curys	Cristianse	задач
115	01.07.2021 10.32.00	Prop	Update#TeDate	Pb.	Толешно		0 0
291	01.07.2021 10.32.00	Pop	UpdateFileData	Pip.	Yoneumo		0 0
176	01.07.3021 10:32:00	Puip	UpdateFileCuta	Weip	Yoteano		0 0
191	01.07.3021 10:32:00	Раф	PareeDecodedData	Fip	Yonewee		0 0
175	01.07.2021 10:32:00	Prap	UpdateFileData	Nat	Toneuro		0 0
175	01.07.2021 10:31:00	Posp	Updote/FieDuta	One	Yoneuro		0 0
115	01.07.202110.31:00	Prop	Updote/FieData	Vieb	Устешно		0 0
115	01.07.2021 10:31:00	Prop	ParaeDecodedData	Pp.	Устешно		0 0
175	01.07.2021 10:31:00	Prop	ParaeDecodedData	Vep	Тотешно	Просмотр информации	
175	01.07.2021 10:31:00	Prop	PerseDecodedDate	That .	Toreano	a salita se	0 0
115	01.07.2021 10.31.00	Prop	ParseDecodedCata	Ons	Tonesare		0 0
115	01.07.2021 10:31:00	Prap	ParseDecodedData	Vieb	Yoreamo		0 0
176	01.07.3021 10:31:00	Рикр	DecoderAction	Fip	Yoheano		0 0
175	01.07.2021 10:31:00	Prap	DecodeAction	Veip	Yonewe		0 0
175	01.07.2021 10:31:00	Prap	DecodeAction	Mail	Yohuno		0 0
115	01.87.2021 18:31:00	Pcap	DecodeAction	One	Услешно		0 0