Содержание

19 Законный перехват	3
Разбор трафика	3
Оборудование	3
Раздел	3
Логи разбора трафика	6

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 8°	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 9	ን ጋ	© СОЕДИНЕНИЯ ГЕНЕРАЦИЯ ТРАФИКА ЗАХВАТ ТРАФИКА		уc	Разбор начат	Разбор заверш
n 11		20	test	John Sn	Û			КЛОНИРОВАНИЕ ВЕБ-САЙТА АУДИТ СЕТИ РАЗБОР ТРАФИКА КАРТА ЗДОРОВЪЯ	,		2 РАЗБОР ТРАФ В ЛОГИ РАЗБОР	ИКА

Раздел Разбора трафика выглядит как на рисунке ниже.

~		~	CKAT DPI	: miniDPI	- 6	0										JS John Smith ~	🗕 RU 🗸 🔡 🥼	۵ 🔍 ۵	v.2.	20.0 5
_	_										Обновит	ьсп	исок			\sim				
-11	3AK	онны	M REPEXEAT / PA	ЗБОР ТРАФИ	COK A	£.			_		фай	лов	ł.							
¢				задам			A	оавить фаи	Ū.			_					Обновить ре	3V0LTAT		
9	3ag	39-04		× 1	0	1	83	adaay				•	Результаты				Concente pe	разбор	~	<
۵	+		Добавление	8	+	ç Oair		Перезапус разбор тра	тить фика			3	Web (49)		🖏 Des (55)	63 Mail (1)	Qu) Valp (0)	D Fi	(35)	3
		10	задачи	Born on	-		in.	для файла	Came	Danfan unur	Barfon same		 Декодированные веб- 	anewerin	ы					
4		10		10012-00			10	01:310:04:27	charge	Peppop Harian	Patoop savepare		Запросы		Изображения					
m				~					~	0	0		B	Mar.						
æ	2	20	test	John Sr 📋		۵	298	minidpi_udpi_1030	anos	30.06.2021 10:31	30.06.2021 10:34	Û	Maria	shu				Pathes	merog	
4	k				12	Δ.	297	udpi_1030120045	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	dr/en/disallowedcertatl.cab	9 667576 0	GET	Ø
Pe	дакт	ир	овать	задач	<u>ر</u>		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/disallowedcertatl.cab	2261fc1 0	GET	Ø
	за,	дач	iy .		2		294	udpi_0525155624_	3eeet	30.06.2021 10:30	30.06.2021 10:32	Û	20.40.2020.00.02.02		in the second se			370		
					12	⇔	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	961	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
					12	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		280	GET	œ
					-								30.10.2020 08:51:00	en kremi	in rahtaticimpiavpivideo.av	19		347	GET	®
					N)	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		126	OFT	
					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		663	OC1	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 ann de			-63	285	udpi_0525156324_	a 3eeet	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	SubisAqJR47S309Riu5bo	EBJKA 388038	GET	0
					8	≙	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 of Garage	wVine	55126	OFT	0
				400	121	۸	281		- Same	38.06.2021 10:50	30.06.2021.10-32	•	39.10.2020 00.21.00	1000.00			ILL WY	55120	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 ПЕРЕХВАТ	/ РАЗБОР ТРАФИК	4		
За,	дачи Доба	вить задачу	Файль	al.	
+	K	S	+	9	
£≣	Задачи 🔍	ома создания	Φ.	айлы	
	ID Задача	задачио		ID	Название
	🗄 Разбор трафия	(a			
	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			
+			C 3ap	ачи				
£≣ 3	Задачи		9	Файлы				
	ID :	Задача	Пользон	ID	Название		Ста	тус
1								÷
	f≣ Pas6	іор трафика				10301		Зав
	Название	e te	st			0046_		Заве
	Описание	e t	lest			r-IEEE		Заве
						p		Заве
						5624_0		Заве
						4024_0		Заве
			Отменить	Co	хранить	pcap		3ano

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

Результаты разбора

Логи разбора трафика

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

_ ≡ -	CKAT DPI : min	DPI	→ ⊙	
З4	АВЛЕНИЕ DPI	•	рафика	
SF ST P	АВЛЕНИЕ УСЛУГАМИ			
₽ 008	АНАЛИТИКА			
🚽 🛆 CEP	BICH VAS CLOUD			
⊸ ⇒ ⇒ зак	ОННЫЙ ПЕРЕХВАТ			Действие
20 АДЛ	ИНИСТРАТОР		ГЕНЕРАЦИЯ ТРАФИКА	
2 >_ SSH	І ТЕРМИНАЛ УСТРОЙСТВА	·	③ ЗАХВАТ ТРАФИКА	UpdateFileData
291	01.07.2021 10:32:00	Pcap	КЛОНИРОВАНИЕ ВЕБ-САЙТА	UpdateFileData
275	01.07.2021 10:32:00	Pcap	品 АУДИТ СЕТИ	
291	01.07.2021 10:32:00	Pcap	😤 РАЗБОР ТРАФИКА 🔹 🕨	😤 РАЗБОР ТРАФИКА
275	01.07.2021 10:32:00	Pcap	☺ КАРТА ЗДОРОВЬЯ	🔬 ЛОГИ РАЗБОРА ТРАФИКА

Раздел Логов разбора трафика выглядит как на рисунке ниже.

аконный	INEPEXBAT / NORM PAS	IGOPA TRADINA				Обновить список задач	-
d Overes	partispa spadowa						Удалия
P(E) C tipenan	Bru C	bes .	Aprile Tator	Ten paultopa	Curys	Classes	задач
215	01.07.2021 10.32.00	Prap	Update# ReData	Pip.	Toneuro		0 0
291	01.07.2021 10.32.00	Puip	UpdateFileCuta	Pip.	Yoteano		
275	01.07.3021 10:32.00	Puip	UpdateFileCuta	Weip	Yoheano		0 0
291	01.07.3021 10:32:00	Puap	ParaeDecodedData	Fip	Yohano		0 0
275	01.87.2021 18:32:00	Ptap	UpdateFieData	Mail	Услевно		0 0
215	01.07.2021 10:31:00	Ptap	Updote/TieData	One	Устано		
215	01.07.2021 10:31:00	Prap	Updote/TieDuta	Web	Точано		
275	01.07.2021 10:31:00	Prap	ParseDecodedData	Pp	Точено		0 0
275	01.07.2021 10.31.00	Pop	ParseDecodedData	Vep	Тетецио	Просмотр информации	
275	01.07.2021 10:31.00	Prop	ParseDecodedData	Mal	Тетецио	o sagase	0 0
215	01.07.2021 10.31.00	Prop	ParseDecodedCata	Ons	Teneuno		0 0
215	01.07.3021 10.31.00	Puip	ParseDecodedData	Viete	Yoheamo		0 0
275	01.07.3021 10:31:00	Puip	DecodeAction	Fip	Yoheano		0 0
375	01.07.302110.31:00	Puap	DecodeAction	Wep	Yohuno		0 0
275	01.07.2021 10:31:00	Ptap	DecodeAction	Mail	Yoneano		0 0
275	01.07.202110.31:00	Prap	DecodeAction	One	Услешно		0 0