RD1034

Как собрать логи сетевого трафика с помощью Wireshark

В рамках диагностики проблем с сетевым подключением специалистам технической поддержки могут дополнительно понадобиться логи сетевого трафика.

Вы можете собрать их с помощью программы Wireshark, выполнив следующие действия:

- 1. Скачайте установочный файл с сайта Wireshark и установите программу.
- 2. Запустите программу и нажмите 🙆.



3. Выберите сетевой интерфейс, с которого нужно собрать логи, и нажмите Старт.

При выборе сетевого интерфейса ориентируйтесь на график активности, либо предварительно выполните команду ipconfig /all и посмотрите, какому интерфейсу соответствует основной IP-адрес компьютера.

Интерфейс	Трафик		Заголовок уровня Link	Смеш	Длина сн	Буфер (М	Режим Мо
Подключение по локал	ьной сети* 8		Ethernet		поию	2	_
Подключение по локал	ьной сети* 7		Ethernet	\checkmark	поию	2	_
> Ethernet0	mand		Ethernet	\checkmark	поию	2	_
Подключение по локал	ьной сети* б	1	Ethernet	\checkmark	поию	2	_
Adapter for loopback tra	ffic capture		BSD loopback	\checkmark	поию	2	_
> Ethernet			Ethernet	\square	поию	2	_
<		_/	<u> </u>		Marca)
Включить смешанный режи	им для всех интерфейсов		λ		Упра	влять Инт	ерфейсами

- 4. Воспроизведите проблему (например, авторизуйтесь на портале и выполните действия в результате которых воспроизводится ошибка).
- 5. Нажмите 📕

_											
4	Захват	из 6 interfaces						22			<
Φ	айл Ре	дактирование	Просмотр	запуск З	ахват Аналі	из Ста	тистика	Телефо	ния		>
		()		😓 🔿 🗟	🕆 🕹 📃	≣®	Q Q				
	Примени	ть дисплейный	фильтр <С	Ctrl-/>							٠
No		Time	Source		Destination	1		Protocol	Length	Info	^
	94060	42.327332						TCP	1514	443 →	4
	94061	42.327332						TLSv1.2	423	Applic	5
	94062	42.327332						тср	60	49591	-
<										,	
>	Frame	1: 54 bytes	on wire (432 bits), !	54 bvtes ca	ptured	(432 b	its) on	interf	face \D	e ^
5	Ethern	et II. Src:					Dst:				1
5	Intern	et Protocol	Version 4	Sec:	D	st:					
i.				,	-					3	- 1
-	_					_					
00	000										
00	010										
00	20										
00	050										
) 🍸 e	5 interfaces: <liv< td=""><td>e capture in pr</td><td>ogress> Паке</td><td>еты: 94062 · По</td><td>оказаны:</td><td>94062 (1</td><td>.00.0%)</td><td>Профил</td><td>ь: Default</td><td>:</td></liv<>	e capture in pr	ogress> Паке	еты: 94062 · По	оказаны:	94062 (1	.00.0%)	Профил	ь: Default	:

6. Нажмите **Файл** → **Сохранить как** и сохраните логи в формате по умолчанию.

📕 *6 interfaces			<u>.</u>			×
Файл Редактирование Просмотр Запуск	Захват Анализ Ст	татистика	Телефо	ния		>>
Открыть	Ctrl+O					
Открыть Недавние	•					+
Объединить			Protocol	Length	Info	^
Импортировать из Шестнадцатеричного Дам	па		ТСР	60	443	
Закрыть	Ctrl+W		TLSv1.2	1514	Ser	
Сохранить	Ctrl+S	.	TCP	1015	496	
Сохранить Как	Ctrl+Shift+S				~	Ť
Набор Файлов	•	(432 bi	lts) on	interf	face \D	e ^
Экспортировать Указанные Пакеты		·				
Экспорт Результатов Анализа Пакетов	•	t: 8080,	Seq: 1	., Ack:	: 1, Le	n Y
Экспортировать Байты Пакета	Ctrl+Shift+X			Е·		
Экспортировать PDUxи в Файл		· (. ·@· · ·	· · · F · ·	•@		
Экспортировать Ключи Сессии TLS		0 · · K · · C ·	y ∙@ · · L	P -		
Экспортировать Объекты	•					
Печать	Ctrl+P					
Выход	Ctrl+Q					
🥘 🌠 wireshark_6_interfacesNC1FV0.pcapn Паке	ты: 106211 • Показаны:	: 106211 (10	0.0%)	Профил	ь: Defaul	t "

7. Добавьте полученные файлы в архив и пришлите на почту hotline@rutoken.ru.