СТЕТОСКОП

Сетевой анализатор нового поколения

Версия 1.5.6

Оглавление

Введение

Stethoscope — это программный анализатор (x86/AMD64) для контроля сетевого трафика компьютеров локальной сети и сети Интернет. Он записывает и анализирует сетевой трафик, в том числе имеет возможность записи открытого SSL/TLS. Программа умеет вести полную запись всего сетевого трафика, либо же выборочную– для анализа только тех данных, которые соответствуют требованиям пользователя. Кроме того, приложение осуществляет индексацию записанного сетевого трафика по отдельным параметрам для упрощения дальнейшего поиска в общем массиве данных.

Stethoscope позволяет находить в сети потенциально уязвимые области, выявлять аномалии и их причины, расследовать сетевые инциденты, вести контроль за сетевой активностью пользователя в Интернете – и все в удобном и интуитивно понятном интерфейсе. Для этого анализируется записанный программой сетевой трафик и ведется сбор статистики по накопленным данным. При этом анализ сетевых взаимодействий может осуществляться ретроспективно – за любой отрезок времени. Программа предоставляет полную картину сетевых потоков, имеет широкие возможности поиска, сортировки и фильтрации данных.

Stethoscope также предоставляет возможность анализировать контент и впоследствии настраивать гибкую систему блокировок и запретов, чтобы избежать утечек информации или, например, нецелевого использования сотрудниками рабочего времени. Программа дает возможности блокирования по заданным фильтрам трафика почты, web-переписки сотрудников, определенного web-контента, вирусов. Приложение осуществляет сохранение объектов – писем, файлов, запросов для последующего анализа контента.

Установщик

Первичная установка

Установка программного комплекса Stethoscope может быть полной или частичной. Частичная установка позволяет установить на компьютер только определённые компоненты, которые впоследствии смогут взаимодействовать с компонентами, установленными на других компьютерах той же сети.

Советы по установке: Убедитесь, что скорость работы диска, на который устанавливается программный комплекс, выше скорости используемого сетевого интерфейса; Старайтесь располагать каталог программ и каталоги хранилища и сетевых данных на разных дисках;

Хранилищу для установки может потребоваться до 2 Гб свободного места на диске.

Компоненты

Первой страницей установщика является страница выбора компонентов.

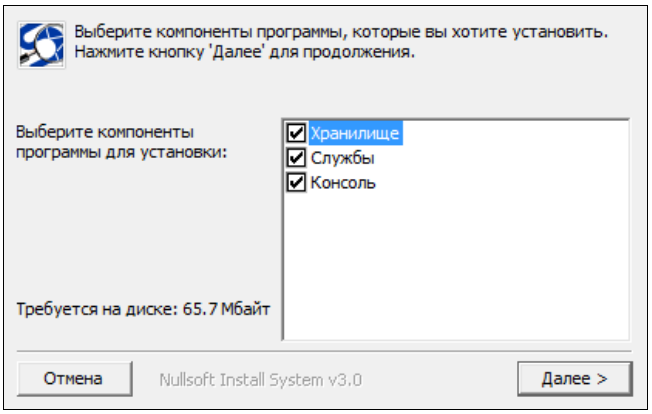


Рис. 1. Окно компонентов

На странице, представленной на Рис. 1**Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.**, галочками отмечаются компоненты, которые необходимо установить.

Хранилище - это база данных postgres, а также необходимые для её работы и взаимодействия с комплексом Stethoscope сервисы.

Службы - это набор сервисов и драйверов, осуществляющих считывание сетевого трафика, его обработку, запись в хранилище, передачу и автоматическую очистку в течение всего времени работы программного комплекса.

Консоль - главное окно пользовательского интерфейса управления комплексом Stethocope.

Таблица подсетей

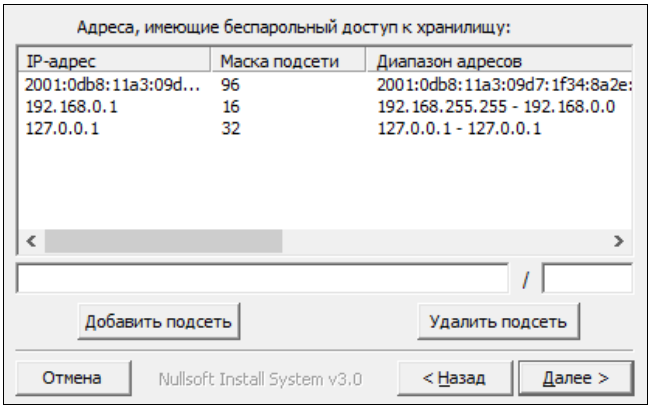


Рис. 2. Окно таблицы подсетей

Страница, представленная на Рис. 2, появляется в том случае, когда на установку помечено исключительно хранилище.

Здесь расположена таблица, в которую можно добавлять подсети, которые будут иметь беспарольный доступ к хранилищу.

Чтобы добавить подсеть в таблицу, необходимо в левом поле ввода указать адрес (поддерживаются как адреса IPv4, так и IPv6), а в правом - маску подсети в числовом виде (от 1 до 32 бит для IPv4, от 1 до 128 для IPv6). После нажатия кнопки [Добавить подсеть], адрес с маской будут добавлены в таблицу, на основе маски будет вычислен диапазон адресов.

Чтобы удалить подсеть, необходимо выделить нужный адрес в таблице и нажать [Удалить подсеть].

Директории установки

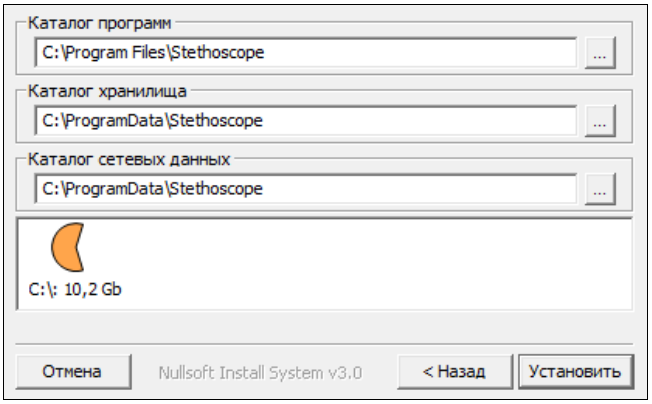


Рис. 3. Окно директорий установки

На странице, представленной на Рис. 3, необходимо указать пути к каталогам для устанавливаемых компонентов. В зависимости от выбранных компонентов, количество и

значение полей ввода на странице может разниться. Под полями ввода отображаются все доступные для установки жесткие диски, а также объём свободного места на каждом из них.

Каталог программ - это каталог, куда будут установлены консоль и сервисы со всеми необходимыми библиотеками и файлами настроек.

Каталог хранилища - это каталог, куда будет установлено хранилище данных, и куда в дальнейшем будут записываться все обработанные данные, полученные в процессе работы Stethoscope.

Каталог сетевых данных - это каталог, куда будут сохраняться необработанные данные, полученные в процессе работы Stethoscope.

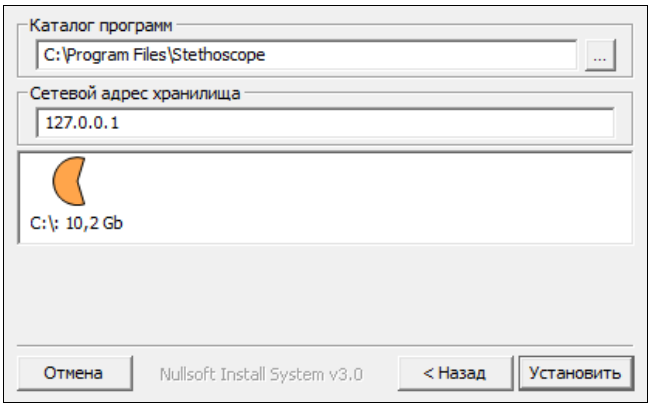


Рис. 4. Окно директорий установки с полем ввода сетевого адреса хранилища

Если хранилище данных не будет устанавливаться, то на данной странице будет присутствовать поле ввода сетевого адреса хранилища, как показано на Рис. 4. В это поле необходимо ввести адрес хранилища, к которому следует подключаться консоли и сервисам.

Обновление

Компоненты программного комплекса Stethoscope могут быть обновлены с помощью исполняемого файла установщика.

Для обновления необходимо запустить установщик, на странице компонентов выбрать компоненты, которые нужно обновить либо установить.

На следующей странице - действия с компонентами - необходимо пометить выбранные компоненты для обновления , выбрав соответствующий пункт, после чего - следовать шагам установщика, как и при первоначальной установке программного комплекса.

Внимание! Обновление некоторых компонентов может потребовать дополнительной перезагрузки в процессе установки.

Действия с компонентами

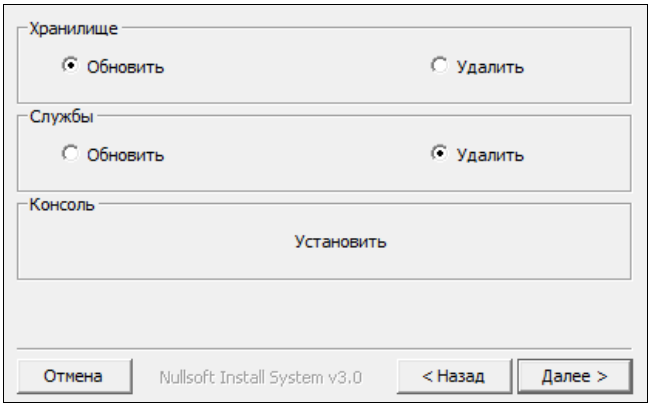


Рис. 5. Окно действий с компонентами

Страница, представленная на Рис. 5, появляется при обновлении через установщик.

Здесь пользователю предоставляется возможность выбрать, что необходимо сделать с выбранными компонентами.

Если компонент ещё не установлен, то он будет помечен на установку. Если компонент уже установлен, то он может быть помечен на обновление либо удаление по желанию пользователя.

Консоль

Окно интерфейса

Валовый график

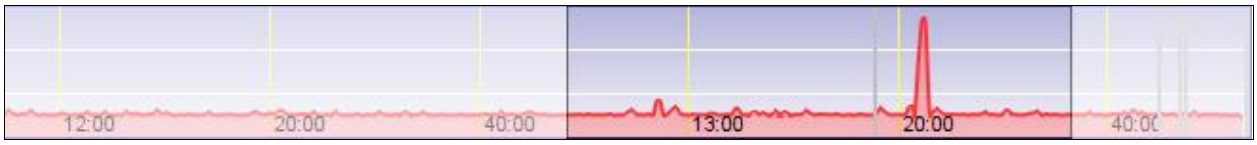


Рис. 6. Валовый график

На валовом графике (Рис. 6) отображаются данные, записанные в хранилище за определённый период времени.

Отображаемый период времени можно настроить, нажав кнопку [Установки времени графика]

Данные, выводимые на график, делятся на *сессии*, *пакеты* и *трафик байтов*. Переключаться между ними можно с помощью выпадающего списка в правом верхнем углу консоли:

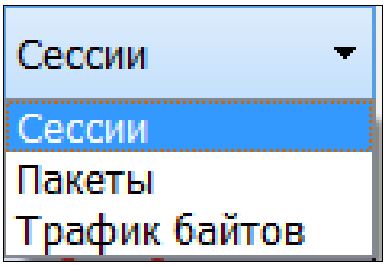


Рис. 7. Выпадающий список выбора данных, отображаемых на валовом графике

На валовом графике можно выставлять линзу, захватывающую только определённый участок графика. Выставить линзу можно, задав её границы в полях, расположенных над валовым графиком (Рис. 8), и нажав кнопку [Применить]:

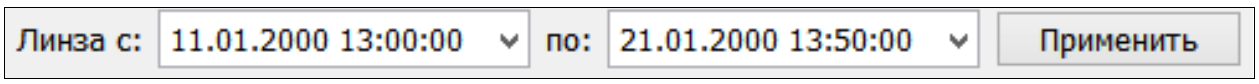


Рис. 8. Поля настройки границ линзы

То же можно сделать с помощью мыши. Для этого необходимо кликнуть курсором мыши на участке графика, который будет являться одной из границ линзы, и, не отпуская левой кнопки мыши, двигать курсор, тем самым выставляя вторую границу линзы.

После этого линзу можно двигать по графику, кликнув по захваченному ею участку и двигая курсор мыши в нужном направлении, не отпуская при этом левой кнопки мыши.

Масштаб валового графика

Справа от валового графика располагаются три переключателя, позволяющие менять масштаб отображения данных на валовом графике:

- Логарифмический масштаб (Рис. 9) – высота пиков на графике усредняется;

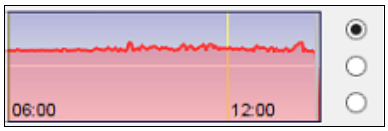


Рис. 9. Валовый график в логарифмическом масштабе

- Увеличенный масштаб (Рис. 10) – верхние пики графика обрезаются с целью сделать мелкие детали заметнее. В данном масштабе так же возможно дополнительное масштабирование с помощью колеса мышки;

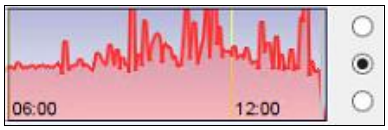


Рис. 10. Валовый график в увеличенном масштабе

- Линейный масштаб (Рис. 11) – график отображается целиком, со всеми верхними границами.

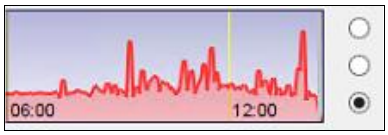


Рис. 11. Валовый график в линейном масштабе

Список процессов

В списке процессов (Рис. 12) отображаются известные процессы (приложения), открывавшие какие-либо сессии из захваченных линзой на валовом графике. Рядом с процессом указывается число сессий/пакетов/байт (в зависимости от выбранного режима отображения валового графика), относящихся к конкретному процессу.

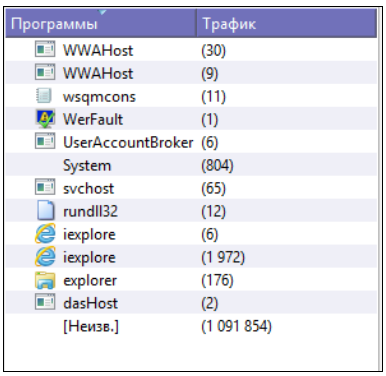


Рис. 12. Список процессов

В списке можно выделить определённый процесс - это отфильтрует список сессий, гистограмму протоколов, таблицу протоколов и линзу, где будут отображены только сессии, соответствующие выбранному процессу.

Для отмены фильтра необходимо щёлкнуть левой кнопкой по пустому месту в списке процессов.

География сетевых соединений

В дереве географии сетевых соединений (Рис. 13) с точностью до города/области отображаются географические адреса, соответствующие IP-адресам, указанным в сессиях, захваченных линзой на валовом графике.

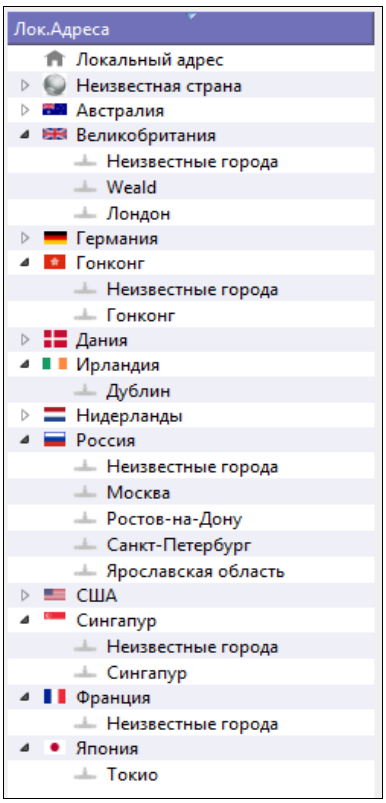


Рис. 13. Дерево географии

В дереве можно выделить определённую страну/город - это отфильтрует список сессий, гистограмму протоколов, таблицу протоколов и линзу, где будут отображены только сессии, соответствующие выбранному адресу.

Для отмены фильтра необходимо щёлкнуть левой кнопкой по пустому месту в дереве географии.

Дерево протоколов

В дереве протоколов (Рис. 14) отображаются все сетевые протоколы, задействованные в сессиях, захваченных линзой на валовом графике.

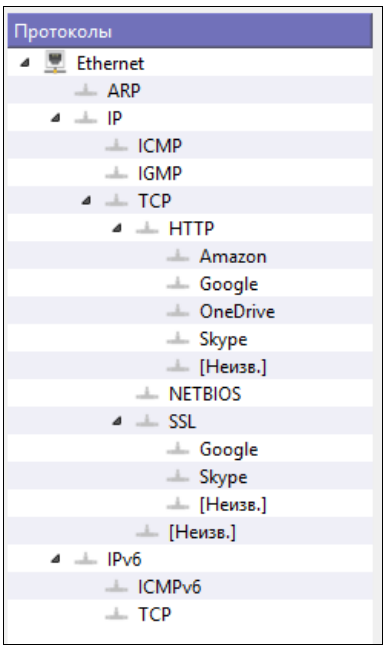


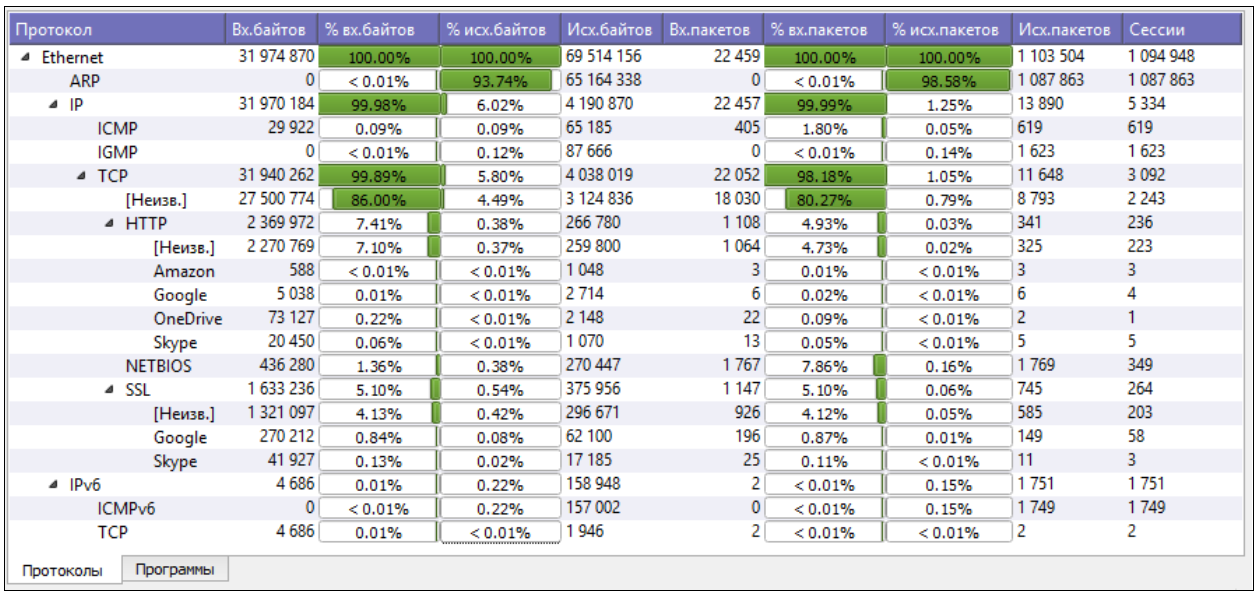
Рис. 14. Дерево протоколов

В дереве можно выделить определённый протокол - это отфильтрует список сессий, гистограмму протоколов, таблицу протоколов и линзу, где будут отображены только сессии, в которых был задействован выбранный протокол.

Для отмены фильтра необходимо щёлкнуть левой кнопкой мыши по пустому месту в дереве протоколов.

Таблица протоколов

В таблице протоколов (Рис. 15) выводится подробная информация о сессиях, захваченных линзой на валовом графике. К этой информации относится количество *входящих\исходящих пакетов*, *входящих\исходящих байт* и *сессий* (в числовом и процентном представлении), приходящиеся на каждый из протоколов, задействованных в захваченных сессиях.



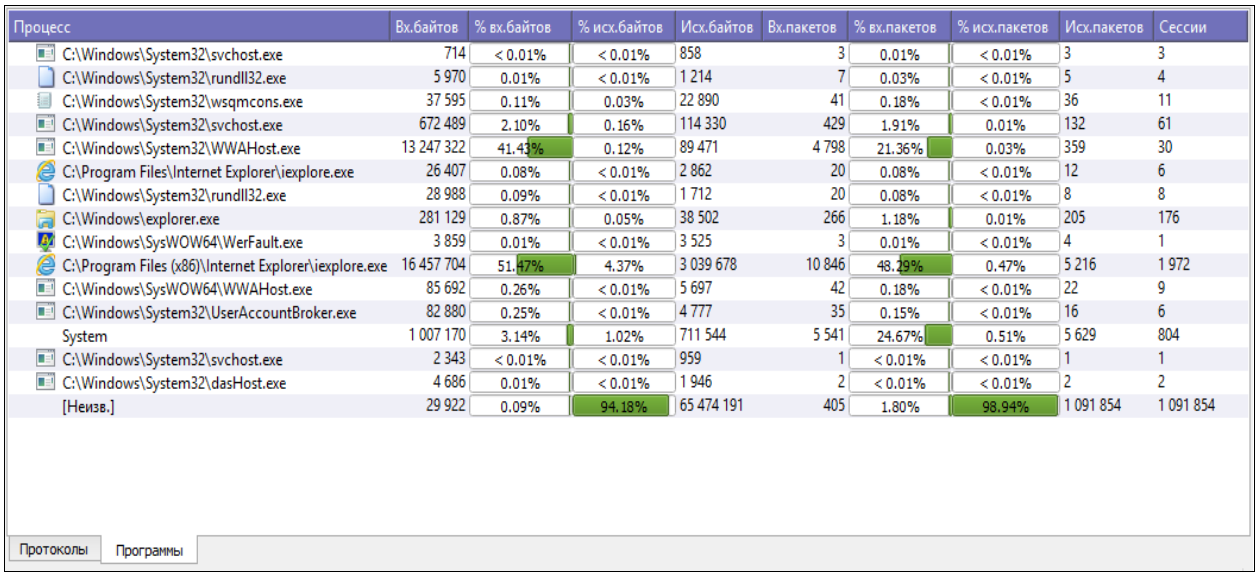
Протокол	Вх.байтов	% вх.байтов	% исх.байтов	Исх.байтов	Вх.пакетов	% вх.пакетов	% исх.пакетов	Исх.пакетов	Сессии
Ethernet	31 974 870	100.00%	100.00%	69 514 156	22 459	100.00%	100.00%	1 103 504	1 094 948
ARP	0	< 0.01%	93.74%	65 164 338	0	< 0.01%	98.58%	1 087 863	1 087 863
IP	31 970 184	99.98%	6.02%	4 190 870	22 457	99.99%	1.25%	13 890	5 334
ICMP	29 922	0.09%	0.09%	65 185	405	1.80%	0.05%	619	619
IGMP	0	< 0.01%	0.12%	87 666	0	< 0.01%	0.14%	1 623	1 623
TCP	31 940 262	99.89%	5.80%	4 038 019	22 052	98.18%	1.05%	11 648	3 092
[Неизв.]	27 500 774	86.00%	4.49%	3 124 836	18 030	80.27%	0.79%	8 793	2 243
HTTP	2 369 972	7.41%	0.38%	266 780	1 108	4.93%	0.03%	341	236
[Неизв.]	2 270 769	7.10%	0.37%	259 800	1 064	4.73%	0.02%	325	223
Amazon	588	< 0.01%	< 0.01%	1 048	3	0.01%	< 0.01%	3	3
Google	5 038	0.01%	< 0.01%	2 714	6	0.02%	< 0.01%	6	4
OneDrive	73 127	0.22%	< 0.01%	2 148	22	0.09%	< 0.01%	2	1
Skype	20 450	0.06%	< 0.01%	1 070	13	0.05%	< 0.01%	5	5
NETBIOS	436 280	1.36%	0.38%	270 447	1 767	7.86%	0.16%	1 769	349
SSL	1 633 236	5.10%	0.54%	375 956	1 147	5.10%	0.06%	745	264
[Неизв.]	1 321 097	4.13%	0.42%	296 671	926	4.12%	0.05%	585	203
Google	270 212	0.84%	0.08%	62 100	196	0.87%	0.01%	149	58
Skype	41 927	0.13%	0.02%	17 185	25	0.11%	< 0.01%	11	3
IPv6	4 686	0.01%	0.22%	158 948	2	< 0.01%	0.15%	1 751	1 751
ICMPv6	0	< 0.01%	0.22%	157 002	0	< 0.01%	0.15%	1 749	1 749
TCP	4 686	0.01%	< 0.01%	1 946	2	< 0.01%	< 0.01%	2	2

Протоколы | Программы

Рис. 15. Таблица протоколов

Таблица процессов

В таблице процессов (Рис. 16) выводится подробная информация о процессах, участвующих в захваченных линзой на валовом графике сессиях. К этой информации относится количество *входящих\исходящих пакетов*, *входящих\исходящих байт* и *сессий* (в числовом и процентном представлении), приходящиеся на каждый из процессов, задействованных в захваченных сессиях.



Процесс	Вх.байтов	% вх.байтов	% исх.байтов	Исх.байтов	Вх.пакетов	% вх.пакетов	% исх.пакетов	Исх.пакетов	Сессии
C:\Windows\System32\svchost.exe	714	< 0.01%	< 0.01%	858	3	0.01%	< 0.01%	3	3
C:\Windows\System32\rundll32.exe	5 970	0.01%	< 0.01%	1 214	7	0.03%	< 0.01%	5	4
C:\Windows\System32\wsqmcons.exe	37 595	0.11%	0.03%	22 890	41	0.18%	< 0.01%	36	11
C:\Windows\System32\svchost.exe	672 489	2.10%	0.16%	114 330	429	1.91%	0.01%	132	61
C:\Windows\System32\WWAHost.exe	13 247 322	41.43%	0.12%	89 471	4 798	21.36%	0.03%	359	30
C:\Program Files\Internet Explorer\iexplore.exe	26 407	0.08%	< 0.01%	2 862	20	0.08%	< 0.01%	12	6
C:\Windows\System32\rundll32.exe	28 988	0.09%	< 0.01%	1 712	20	0.08%	< 0.01%	8	8
C:\Windows\explorer.exe	281 129	0.87%	0.05%	38 502	266	1.18%	0.01%	205	176
C:\Windows\SysWOW64\WerFault.exe	3 859	0.01%	< 0.01%	3 525	3	0.01%	< 0.01%	4	1
C:\Program Files (x86)\Internet Explorer\iexplore.exe	16 457 704	51.47%	4.37%	3 039 678	10 846	48.29%	0.47%	5 216	1 972
C:\Windows\SysWOW64\WWAHost.exe	85 692	0.26%	< 0.01%	5 697	42	0.18%	< 0.01%	22	9
C:\Windows\System32\UserAccountBroker.exe	82 880	0.25%	< 0.01%	4 777	35	0.15%	< 0.01%	16	6
System	1 007 170	3.14%	1.02%	711 544	5 541	24.67%	0.51%	5 629	804
C:\Windows\System32\svchost.exe	2 343	< 0.01%	< 0.01%	959	1	< 0.01%	< 0.01%	1	1
C:\Windows\System32\dasHost.exe	4 686	0.01%	< 0.01%	1 946	2	< 0.01%	< 0.01%	2	2
[Неизв.]	29 922	0.09%	94.18%	65 474 191	405	1.80%	98.94%	1 091 854	1 091 854

Протоколы | Программы

Рис. 16. Таблица процессов

Гистограмма протоколов

На гистограмме протоколов (Рис. 17) наглядно показано количество всех сетевых протоколов, задействованных в сессиях, захваченных линзой на валовом графике.

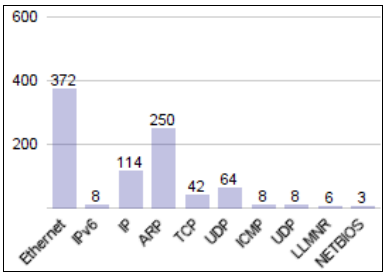


Рис. 17. Гистограмма протоколов

Линза валового графика

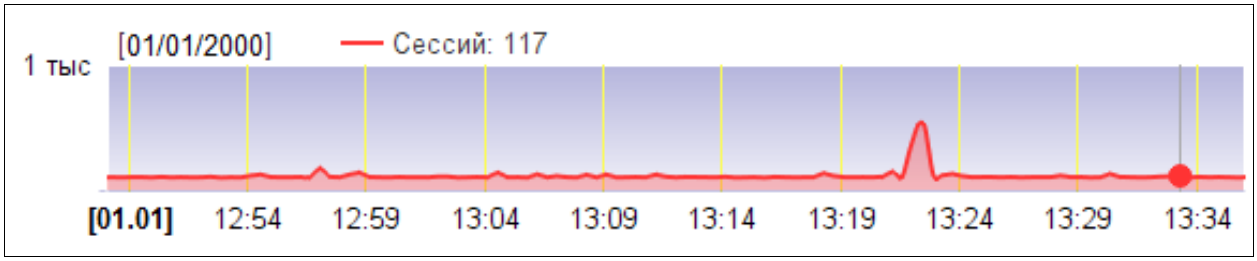


Рис. 18. Линза валового графика

Линза валового графика (Рис. 18) - это захваченный участок валового графика, фильтруемый с помощью списка процессов, дерева протоколов, географии сетевых процессов, таблицы протоколов и гистограммы протоколов.

В окне линзы отображается увеличенный участок валового графика, дата и время выделенного участка, а также, в зависимости от отображаемой на валовом графике информации, количество *сессий*, *входящих/исходящих пакетов* или *входящих/исходящих байт* в выбранной на линзе точке времени.

Панель управления

О программе

Нажатие на кнопку  - [О программе] приводит к открытию окна, показанного на Рис. 19, содержащего зарегистрированный логотип консоли, её текущую версию, сведения о фирме-разработчике и ссылку на сайт разработчика.

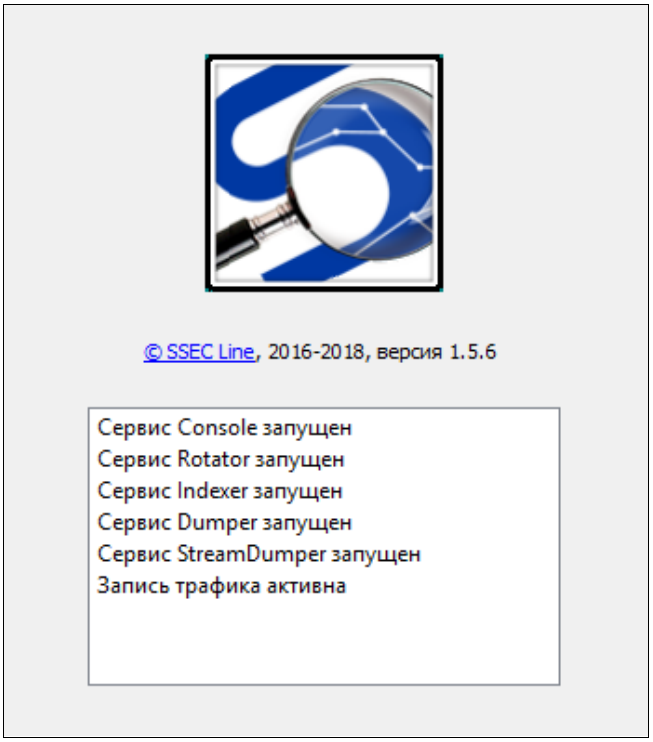


Рис. 19. Окно с информацией о консоли

Здесь же расположена информация о работе установленных служб.

Выбор сетевых интерфейсов

Нажатие на кнопку  - [Выбор сетевых интерфейсов] приводит к появлению диалога, представленного на Рис. 20, в котором перечислены все обнаруженные сетевые интерфейсы компьютера. В данном диалоге необходимо отметить, с каких именно сетевых интерфейсов будут записываться данные.

Для этого следует выбрать необходимые интерфейсы, отметив их галочкой, после чего нажать [Использовать].

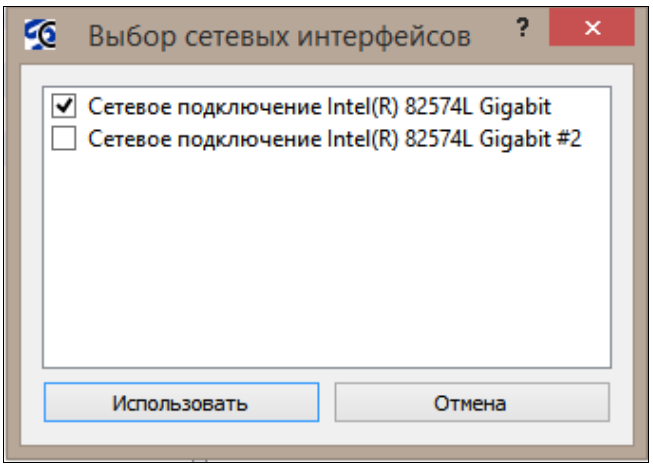


Рис. 20. Окно выбора сетевых интерфейсов

Подключение к БД

Нажатие на кнопку  - [Подключение к БД] приводит к появлению окна, показанного на Рис. 21, - диалога подключения к хранилищу (базе данных), из которого следует брать данные для работы.

Для подключения необходимо: Ввести IP-адрес хранилища в поле *Хост*, Указать *порт* соединения, и ввести *имя пользователя* и *пароль* в соответствующие поля. Далее следует нажать кнопку [Соединение], после чего консоль попытается установить соединение с хранилищем на указанных адресе/порте от имени указанного пользователя.

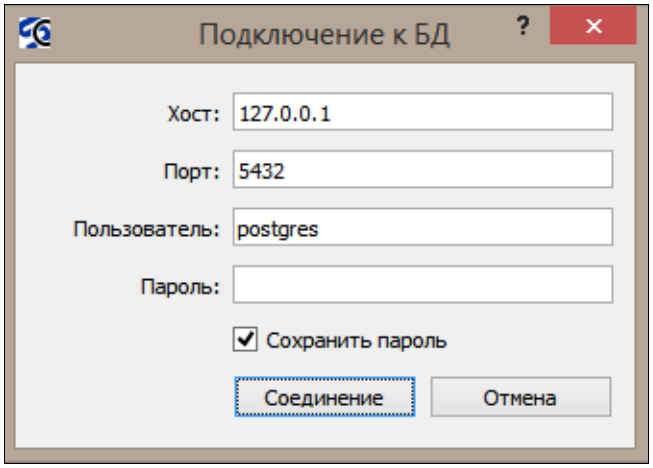


Рис. 21. Окно подключения к хранилищу

Чтобы при последующих попытках соединения не пришлось заново вводить данные пользователя, можно отметить галочкой пункт *Сохранить пароль*.

Установки времени графика

Нажатие на кнопку  - [Установки времени графика] приводит к появлению диалога, представленного на Рис. 22, позволяющего настроить то, поступившие за какой период в хранилище данные отображать на валовом графике.

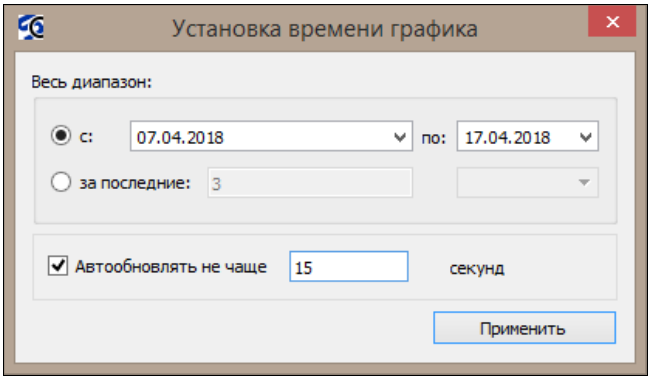


Рис. 22. Окно установок времени графика

Отображение можно настроить двумя способами:

1. Отобразить данные, поступившие в хранилище за определённый *календарный период* (Рис. 23).

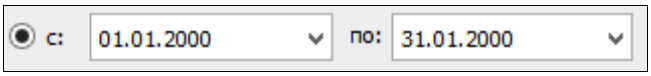


Рис. 23. Поля настройки вывода данных за определённый календарный период

2. Отобразить данные, поступившие в хранилище за определённый *временной период*. На выбор предоставляются следующие единицы времени: минуты, часы, дни, недели и месяцы (**Ошибка! Источник ссылки не найден.**).

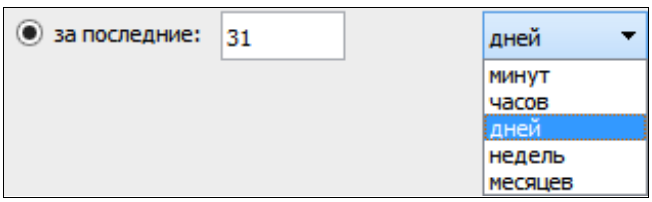


Рис. 24. Поля настройки вывода данных за определённый временной период

Внимание! Минимально допустимый период - 12 минут!

Режим автообновления

В режиме автообновления данные на валовом графике будут обновляться с периодичностью, заданной пользователем. Для включения режима автообновления нужно отметить его галочкой и выставить частоту обновления (по умолчанию - раз в 15 секунд).

Настройки

Нажатие на кнопку - [Настройки] приводит к появлению диалога, показанного на Рис. 25, позволяющего настроить различные параметры программного комплекса Stethoscope.

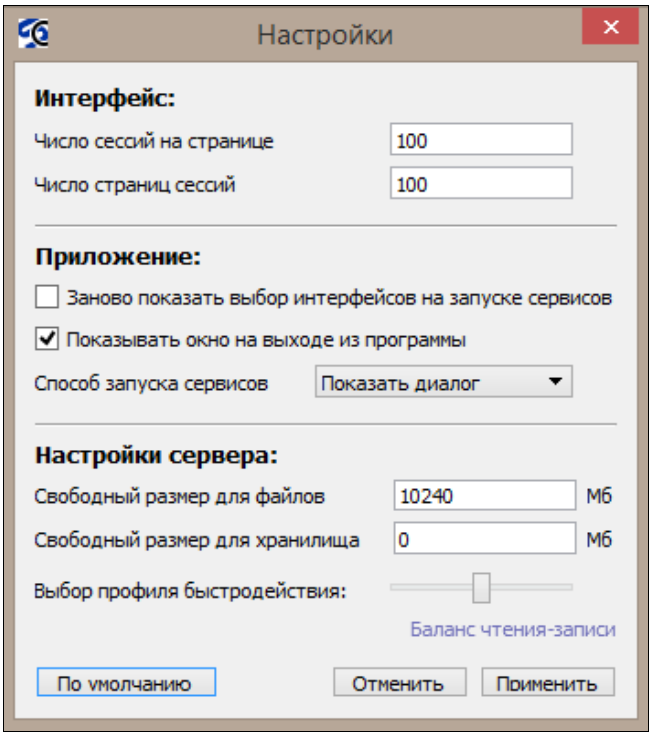


Рис. 25. Окно настроек

Блок **Интерфейс** содержит 2 поля: *Число сессий на странице* - количество сессий, отображаемых на одной странице в окне сессий; *Число страниц сессий* – максимально допустимое количество страниц сессий, отображаемых в окне сессий.

Блок **Приложение** позволяет настроить поведение консоли при запуске и закрытии. *Заново показать выбор интерфейсов на запуске сервисов* при следующем нажатии на кнопку [Запустить просмотр] откроет диалог выбора сетевых интерфейсов. *Показывать окно на выходе из программы* открывает диалог, представленный на Рис. 26, где работа сервисов программного комплекса может быть как остановлена, так и продолжена при завершении работы консоли.

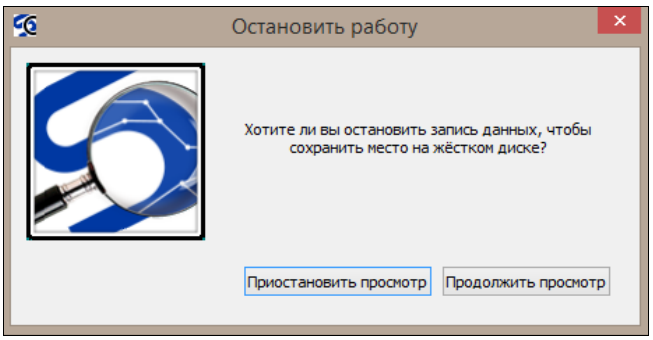


Рис. 26. Окно остановки работы

За работу сервисов также отвечает параметр *Способ запуска сервисов*, где может быть изменён выбор, сделанный в диалоге закрытия консоли (Рис. 27).

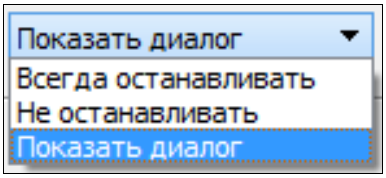


Рис. 27. Способ запуска сервисов

Блок **Настройки сервера** содержит 2 поля: *Свободный размер для файлов* - максимально допустимый суммарный размер хранящихся на диске nsc- и pcap-файлов, при достижении которого будут удаляться более старые файлы; *Свободный размер для хранилища* - максимально допустимый размер хранилища (базы данных), при достижении которого будут удаляться более старые записи; и ползунок *Выбор профиля быстродействия*, имеющий три положения: *Оптимизировать на запись* - данные будут записываться в хранилище с максимальной скоростью при пониженной нагрузке на систему и низкой скорости обновления данных в консоли; *Баланс чтения-записи* – сбалансированный профиль со средней нагрузкой на систему; *Оптимизировать на чтение* - высокая корость обновления данных в консоли при высокой нагрузке на процессор и жесткий диск системы.

Запустить просмотр

Нажатие на кнопку - [Запустить просмотр] приводит к запуску службы, записывающей весь трафик в хранилище для дальнейшей работы с ним.

Если консоль запущена в первый раз, то при нажатии на кнопку [Запустить просмотр] будет открыт диалог выбора сетевых интерфейсов, так как сервису ещё не известно, с какого интерфейса следует записывать трафик.

Приостановить просмотр

Нажатие на кнопку - [Приостановить просмотр] приводит к приостановке работы службы, записывающей весь трафик в хранилище для дальнейшей работы с ним. В этом

случае новые данные перестанут поступать в хранилище, однако возможность работы с уже записанными данными останется.

Накопительный режим

Нажатие на кнопку  - [Накопительный режим] приводит к включению автообновления и перемещает линзу к правому краю валового графика. Далее, каждый раз при обновлении данных на валовом графике, линза будет увеличиваться в размерах, захватывая все новые входящие данные, не теряя при этом данные, захваченные линзой ранее.

Фиксированный режим

Нажатие на кнопку  - [Фиксированный режим] приводит к включению автообновления и перемещает линзу к правому краю валового графика. Далее линза будет зафиксирована в этом положении. При этом ранее захваченные данные будут постепенно уступать место новым в рамках линзы.

Сессии

Нажатие на кнопку  - [Сессии] приводит к открытию нового окна, показанного на Рис. 28, которое содержит дерево фильтров сессий, список сессий и информацию о фильтрах сессий.

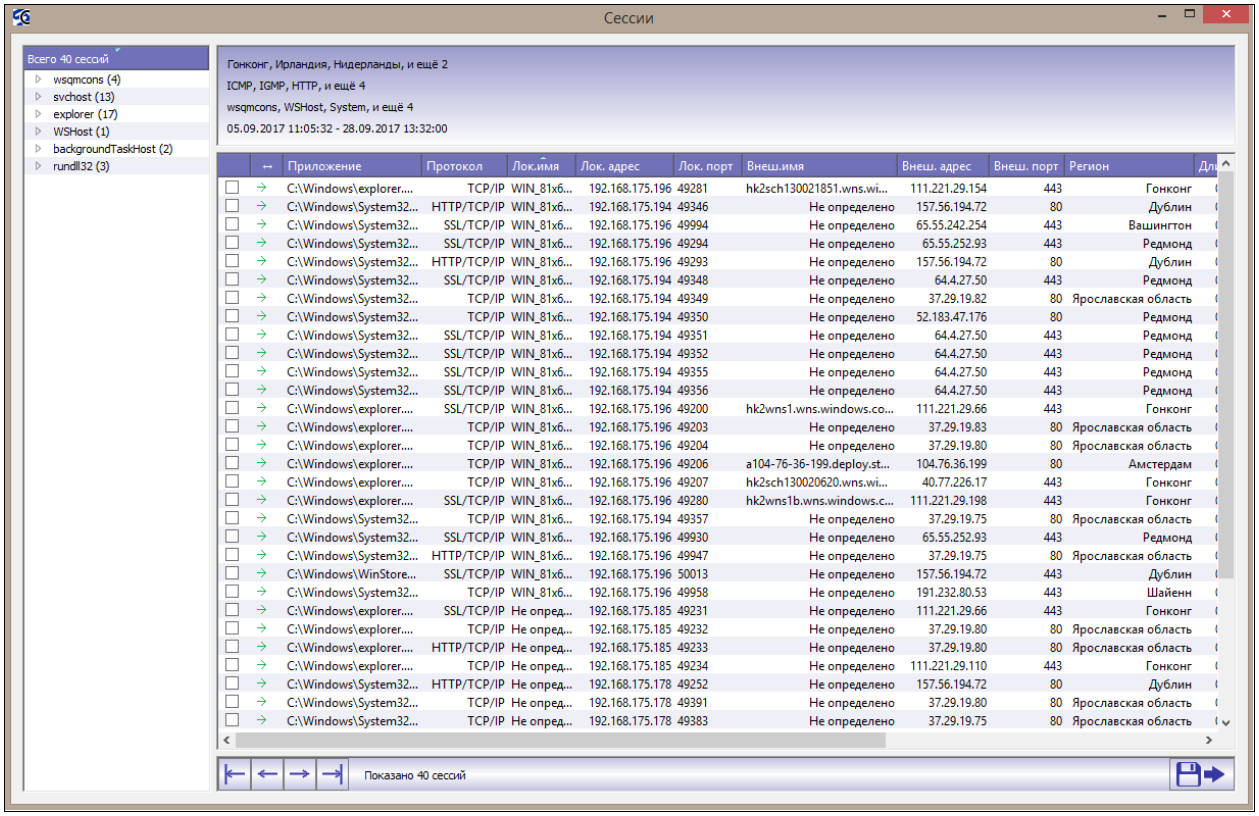


Рис. 28. Окно сессий

Дерево фильтрации сессий

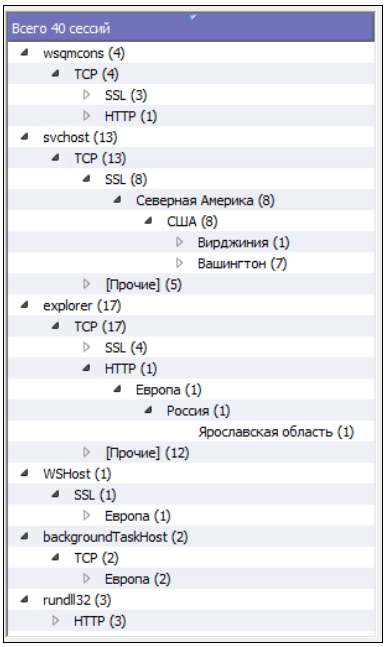


Рис. 29. Дерево фильтрации сессий

Слева от списка сессий находится дополнительное дерево фильтров (Рис. 29), содержащее выбранные процессы.

Процессы могут быть развёрнуты на относящиеся к ним протоколы.

Протоколы, в свою очередь, могут быть развёрнуты на относящуюся к ним географию.

В скобках после каждого пункта показано число сессий, попадающих под фильтрацию с учётом этого и вышележащих пунктов, а также фильтров в главном окне (если есть).

Информация о фильтрах сессий

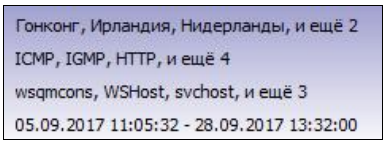
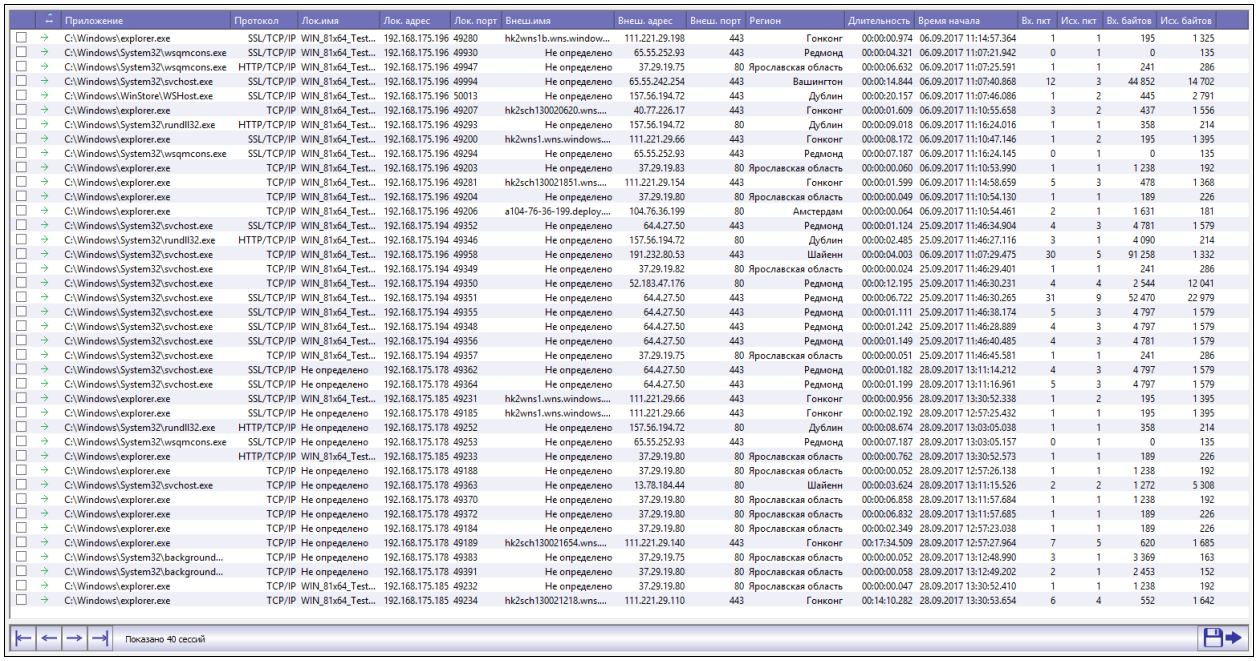


Рис. 30. Информация о фильтрах сессий

Над списком сессий отображается вся информация о текущих выбранных фильтрах сессий, а именно: фильтрация по географии; фильтрация по протоколам; фильтрация по процессам; временной интервал линзы. (Рис. 30)

Список сессий

В списке сессий, показанном на Рис. 31, отображаются все сессии, захваченные линзой на валовом графике, с подробной информацией по каждой сессии: *Чекбокс* (галочка) для отметки сессий на экспорт; *Тип* сессии - исходящая или входящая; *Приложение*, открывшее сессию; (только для локальной версии программы) *Протокол*, задействованный в сессии; *Локальное имя* - сетевое имя компьютера, *с* которого зарегистрирована сессия (локальный текстовой адрес сессии); *Локальный адрес* - сетевой адрес компьютера, *с* которого зарегистрирована сессия (локальный цифровой адрес сессии); *Локальный порт* сессии; *Внешнее имя* - сетевое имя удаленного компьютера (внешний текстовой адрес сессии); *Внешний адрес* - сетевой адрес удаленного компьютера (внешний цифровой адрес сессии); *Внешний порт* сессии; Географический *регион* (поле может отсутствовать); *Время начала* сессии; *Длительность* сессии; Количество *входящих байт*; Количество *исходящих байт*. Количество *входящих пакетов*; Количество *исходящих пакетов*.



	Приложение	Протокол	Лок.имя	Лок. адрес	Лок. порт	Внеш.имя	Внеш. адрес	Внеш. порт	Регион	Длительность	Время начала	Вх. пкт	Исх. пкт	Вх. байтов	Исх. байтов
	C:\Windows\explorer.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	49280	hk2wns1b.wns.window...	111.221.29.198	443	Гонконг	00:00:00.974	06.09.2017 11:14:57.364	1	1	195	1 325
	C:\Windows\System32\wsqmcons.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	49930	Не определено	65.55.252.93	443	Редмонд	00:00:04.321	06.09.2017 11:07:21.942	0	1	0	135
	C:\Windows\System32\wsqmcons.exe	HTTP/TCP/IP	WIN_81x64_Test...	192.168.175.196	49947	Не определено	37.29.19.75	80	Ярославская область	00:00:06.632	06.09.2017 11:07:25.591	1	1	241	286
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	49994	Не определено	65.55.242.254	443	Вашингтон	00:00:14.844	06.09.2017 11:07:40.868	12	3	44 852	14 702
	C:\Windows\WinStore\WSHost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	50013	Не определено	157.56.194.72	443	Дублин	00:00:20.157	06.09.2017 11:07:46.086	1	2	445	2 791
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49207	hk2sch130020620.wns....	40.77.226.17	443	Гонконг	00:00:01.609	06.09.2017 11:10:55.658	3	2	437	1 556
	C:\Windows\System32\rundll32.exe	HTTP/TCP/IP	WIN_81x64_Test...	192.168.175.196	49293	Не определено	157.56.194.72	80	Дублин	00:00:09.018	06.09.2017 11:16:24.016	1	1	358	214
	C:\Windows\explorer.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	49200	hk2wns1.wns.windows....	111.221.29.66	443	Гонконг	00:00:08.172	06.09.2017 11:10:47.146	1	2	195	1 395
	C:\Windows\System32\wsqmcons.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.196	49294	Не определено	65.55.252.93	443	Редмонд	00:00:07.187	06.09.2017 11:16:24.145	0	1	0	135
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49203	Не определено	37.29.19.83	80	Ярославская область	00:00:00.060	06.09.2017 11:10:53.990	1	1	1 238	192
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49281	hk2sch130021851.wns....	111.221.29.154	443	Гонконг	00:00:01.599	06.09.2017 11:14:58.659	5	3	478	1 368
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49204	Не определено	37.29.19.80	80	Ярославская область	00:00:00.049	06.09.2017 11:10:54.130	1	1	189	226
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49206	a104-76-36-199.deploy....	104.76.36.199	80	Амстердам	00:00:00.064	06.09.2017 11:10:54.461	2	1	1 631	181
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.194	49352	Не определено	64.4.27.50	443	Редмонд	00:00:01.124	25.09.2017 11:46:34.904	4	3	4 781	1 579
	C:\Windows\System32\rundll32.exe	HTTP/TCP/IP	WIN_81x64_Test...	192.168.175.194	49346	Не определено	157.56.194.72	80	Дублин	00:00:02.485	25.09.2017 11:46:27.116	3	1	4 090	214
	C:\Windows\System32\svchost.exe	TCP/IP	WIN_81x64_Test...	192.168.175.196	49958	Не определено	191.232.80.53	443	Шайенн	00:00:04.003	06.09.2017 11:07:29.475	30	5	91 258	1 332
	C:\Windows\System32\svchost.exe	TCP/IP	WIN_81x64_Test...	192.168.175.194	49349	Не определено	37.29.19.82	80	Ярославская область	00:00:00.024	25.09.2017 11:46:29.401	1	1	241	286
	C:\Windows\System32\svchost.exe	TCP/IP	WIN_81x64_Test...	192.168.175.194	49350	Не определено	52.183.47.176	80	Редмонд	00:00:12.195	25.09.2017 11:46:30.231	4	4	2 544	12 041
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.194	49351	Не определено	64.4.27.50	443	Редмонд	00:00:06.722	25.09.2017 11:46:30.265	31	9	52 470	22 979
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.194	49355	Не определено	64.4.27.50	443	Редмонд	00:00:01.111	25.09.2017 11:46:38.174	5	3	4 797	1 579
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.194	49348	Не определено	64.4.27.50	443	Редмонд	00:00:01.242	25.09.2017 11:46:28.889	4	3	4 797	1 579
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.194	49356	Не определено	64.4.27.50	443	Редмонд	00:00:01.149	25.09.2017 11:46:40.485	4	3	4 781	1 579
	C:\Windows\System32\svchost.exe	TCP/IP	WIN_81x64_Test...	192.168.175.194	49357	Не определено	37.29.19.75	80	Ярославская область	00:00:00.051	25.09.2017 11:46:45.581	1	1	241	286
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	Не определено	192.168.175.178	49362	Не определено	64.4.27.50	443	Редмонд	00:00:01.182	28.09.2017 13:11:14.212	4	3	4 797	1 579
	C:\Windows\System32\svchost.exe	SSL/TCP/IP	Не определено	192.168.175.178	49364	Не определено	64.4.27.50	443	Редмонд	00:00:01.199	28.09.2017 13:11:16.961	5	3	4 797	1 579
	C:\Windows\explorer.exe	SSL/TCP/IP	WIN_81x64_Test...	192.168.175.185	49231	hk2wns1.wns.windows....	111.221.29.66	443	Гонконг	00:00:00.956	28.09.2017 13:30:52.338	1	2	195	1 395
	C:\Windows\explorer.exe	SSL/TCP/IP	Не определено	192.168.175.178	49185	hk2wns1.wns.windows....	111.221.29.66	443	Гонконг	00:00:02.192	28.09.2017 12:57:25.432	1	1	195	1 395
	C:\Windows\System32\rundll32.exe	HTTP/TCP/IP	Не определено	192.168.175.178	49252	Не определено	157.56.194.72	80	Дублин	00:00:08.674	28.09.2017 13:03:05.038	1	1	358	214
	C:\Windows\System32\wsqmcons.exe	SSL/TCP/IP	Не определено	192.168.175.178	49253	Не определено	65.55.252.93	443	Редмонд	00:00:07.187	28.09.2017 13:03:05.157	0	1	0	135
	C:\Windows\explorer.exe	HTTP/TCP/IP	WIN_81x64_Test...	192.168.175.185	49233	Не определено	37.29.19.80	80	Ярославская область	00:00:00.762	28.09.2017 13:30:52.573	1	1	189	226
	C:\Windows\explorer.exe	TCP/IP	Не определено	192.168.175.178	49188	Не определено	37.29.19.80	80	Ярославская область	00:00:00.052	28.09.2017 12:57:26.138	1	1	1 238	192
	C:\Windows\System32\svchost.exe	TCP/IP	Не определено	192.168.175.178	49363	Не определено	13.78.184.44	80	Шайенн	00:00:03.624	28.09.2017 13:11:15.526	2	2	1 272	5 308
	C:\Windows\explorer.exe	TCP/IP	Не определено	192.168.175.178	49370	Не определено	37.29.19.80	80	Ярославская область	00:00:06.858	28.09.2017 13:11:57.684	1	1	1 238	192
	C:\Windows\explorer.exe	TCP/IP	Не определено	192.168.175.178	49372	Не определено	37.29.19.80	80	Ярославская область	00:00:06.832	28.09.2017 13:11:57.685	1	1	189	226
	C:\Windows\explorer.exe	TCP/IP	Не определено	192.168.175.178	49184	Не определено	37.29.19.80	80	Ярославская область	00:00:02.349	28.09.2017 12:57:23.038	1	1	189	226
	C:\Windows\explorer.exe	TCP/IP	Не определено	192.168.175.178	49189	hk2sch130021654.wns....	111.221.29.140	443	Гонконг	00:17:34.509	28.09.2017 12:57:27.964	7	5	620	1 685
	C:\Windows\System32\background...	TCP/IP	Не определено	192.168.175.178	49383	Не определено	37.29.19.75	80	Ярославская область	00:00:00.052	28.09.2017 13:12:48.990	3	1	3 369	163
	C:\Windows\System32\background...	TCP/IP	Не определено	192.168.175.178	49391	Не определено	37.29.19.80	80	Ярославская область	00:00:00.058	28.09.2017 13:12:49.202	2	1	2 453	152
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.185	49232	Не определено	37.29.19.80	80	Ярославская область	00:00:00.047	28.09.2017 13:30:52.410	1	1	1 238	192
	C:\Windows\explorer.exe	TCP/IP	WIN_81x64_Test...	192.168.175.185	49234	hk2sch130021218.wns....	111.221.29.110	443	Гонконг	00:14:10.282	28.09.2017 13:30:53.654	6	4	552	1 642

Показано 40 сессий

Рис. 31. Список сессий

Под списком сессий расположена панель с кнопками, отображающая общее количество выбранных сессий и позволяющая переключаться между страницами с сессиями (если сессий больше 100) или между сессиями при отображении их контента.

Фильтрация

Список сессий можно фильтровать, используя для этого список процессов, дерево географии сетевых подключений, гистограмму протоколов и таблицу протоколов.

Контент

Двойной клик мышкой по одной конкретной сессии показывает её контент – содержимое сессии (Рис. 32).

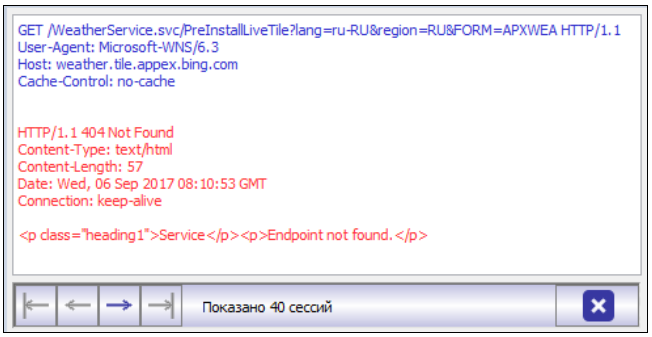


Рис. 32. Контент сессии

Кнопки со стрелками влево  и вправо  при открытой области просмотра контента меняют своё назначение и позволяют двигаться по сессиям, у которых отображается контент (в пределах одной текущей страницы списка сессий). Контент сессий не разделяется на смысловые категории и показываются блоками по 1 килобайту, начиная с каждой смены направлений (входящие-исходящие). В окне не отображаются некоторые специальные символы, поэтому (если надо получить точное содержимое сессий), то следует воспользоваться функцией экспорта в файл. После каждого блока может появиться символ многоточия в угловых скобках (...) который означает, что данный блок можно докачать для просмотра.

Контент исходящих пакетов отображается синим цветом, входящих - красным. Отметка в левой колонке (галка) предназначена для выбора одной или нескольких сессий, содержимое которых можно экспортировать в файл (в формате PCAP). Если ни одна сессия не отмечена, то происходит экспорт не контента, а только списка всех сессий (в формат CSV). Для экспорта списка или контента сессий в файл надо нажать на кнопку  . Для закрытия окна просмотра контента используется кнопка  . Также просмотр закроется автоматически, если изменить фильтрацию (в дереве слева или в главном окне), т.к. список сессий в этом случае поменяется.

Поиск

Нажатие Ctrl+F открывает область поиска по отображаемому контенту. Внимание: поиск ищет только по тому, что вы видите в области просмотра, а не по скрытой (и ещё не показанной) части сессии. Если нужно искать по всему объёму сессии, то следует воспользоваться функцией выгрузки в файл и другими специальными средствами.

Деинсталляция

Деинсталляция программного комплекса Stethoscope может быть как частичной, так и полной.

Для полной деинсталляции необходимо выбрать программный комплекс Stethoscope в "Программах и компонентах" и нажать [Удалить] или запустить исполняемый файл Uninstall.exe из директории установки программного комплекса. Весь последующий процесс не потребует от пользователя никаких действий, кроме подтверждения перезагрузки по окончании деинсталляции.

Частичная деинсталляция является частью функции обновления, осуществляемой с помощью исполняемого файла установщика. Для частичной деинсталляции необходимо запустить установщик, на странице компонентов выбрать компоненты, которые нужно деинсталлировать. На следующей странице - действия с компонентами - необходимо пометить выбранные компоненты на удаление, выбрав соответствующий пункт, после чего - просто нажимать [Далее].

О программе

Версия: 1.5.6

Разработчик: ssecline.ru

Контакты: support@ssecline.ru