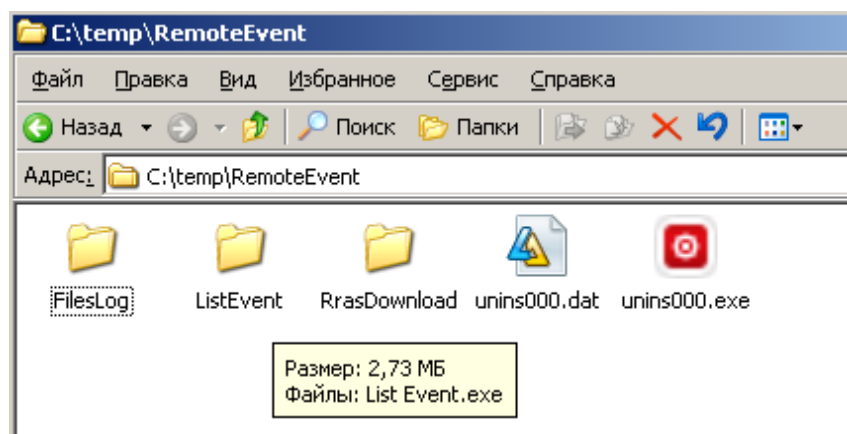


## Руководство администратора по RemoteEvent

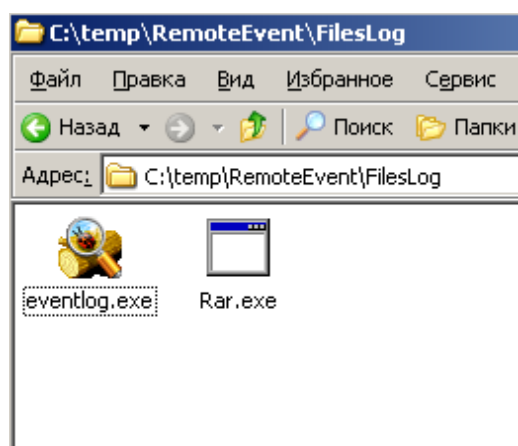
После установке программы в каталоге RemoteEvent создается три папки

1. FilesLog
2. RrasDownload
3. ListEvent



### 1. FilesLog

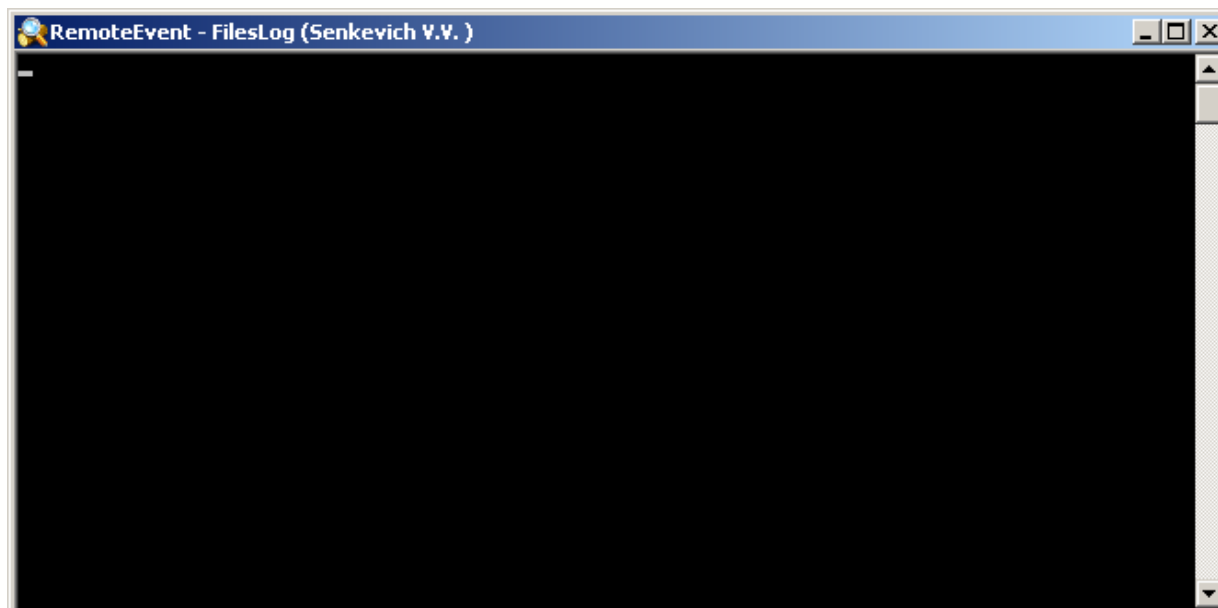
Внутри папки находятся программа [eventlog.exe](#) и архиватор [rar.exe](#)



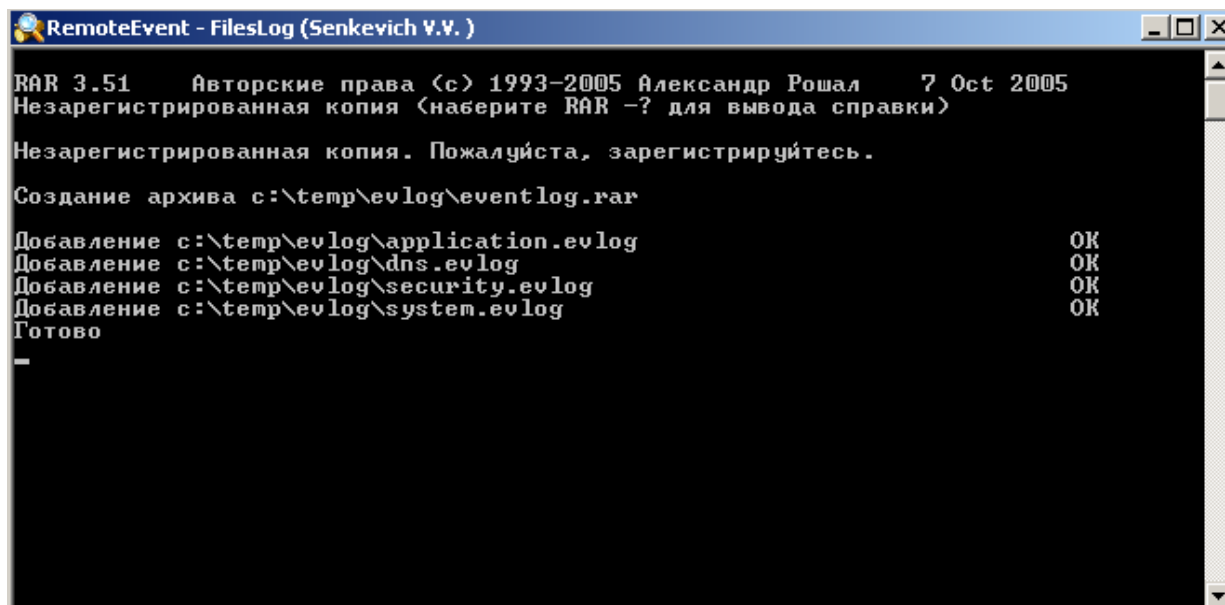
Будет запускаться на удаленных серверах, время запуска назначается в назначенных заданиях. Программа собирает информацию с event log. Журналы – Application, Security, System, Dns.

- 1 – Уведомление
- 2 – Дата
- 3 – Время
- 4 – Источник
- 5 - Код ID
- 6 – Описание

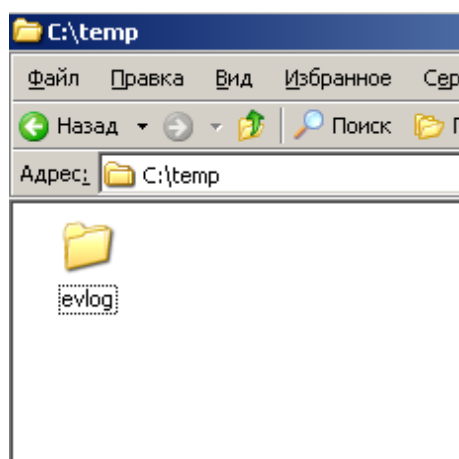
## Тестируем запуск evenlog.exe



После этого запускается архиватор RAR, который сжимает файлы журналов в архив и ложит его `c:\temp\evlog\eventlog.rar`

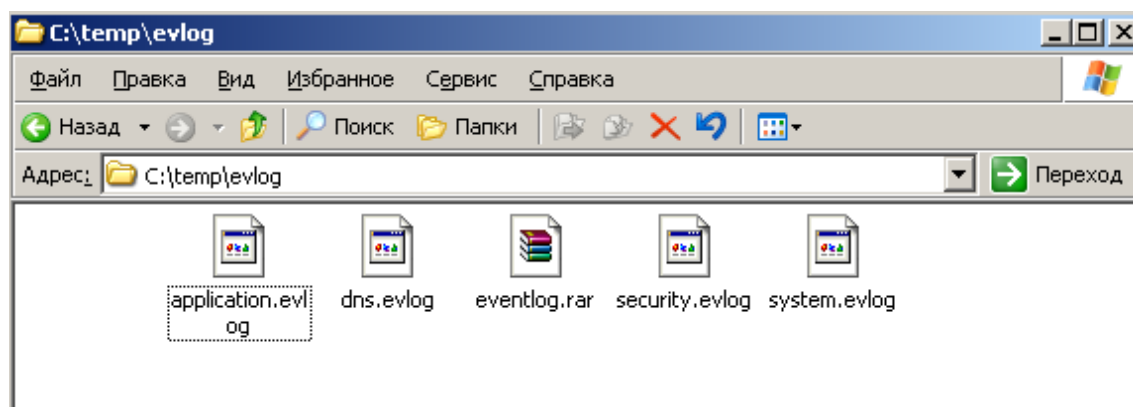


Когда программа закончит свою работу на диске C в каталоге Temp, создаться папка evlog

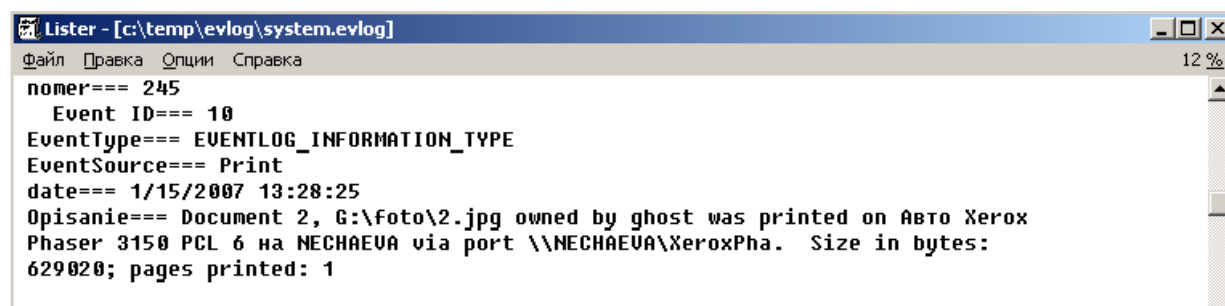


Внутри папки evlog находятся файлы(вносить изменения в файлы строго запрещено) соданные с Просмотра событий:

- system.evlog
- security.evlog
- dns.evlog
- application.evlog
- eventlog.rar(файл для передачи)



Разберем например кусок файла system.evlog



номер – номер события в системе (245)

Event ID - код ошибки (10)

EventType – тип события (Уведомление)

EventSource – источник события (Принтер)

date – дата и время события (1/15/2007 13:28:25)

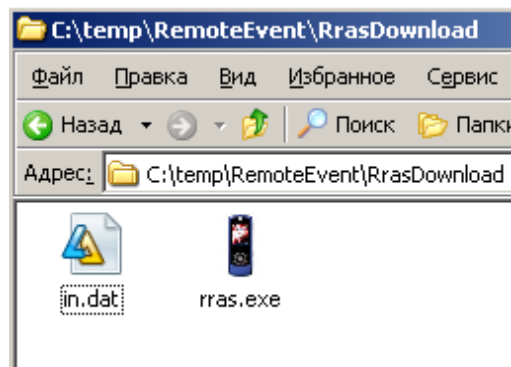
Opisanie – описание события (Документ 2, G:\foto\2.jpg владельца ghost напечатан на Авто Xerox Phaser 3150 PCL 6 на NECHAEVA через порт \\NECHAEVA\XeroxPha. Размер: 629020 байт;

число страниц: 1)

В конце каждого события присутствует уникальный идентификатор `end===endEvent`, он нужен для программы ListEvent

## 2. RrasDownload

Внутри папки находится программа [rras.exe](#) и файл [in.dat](#)



Запускаться на главном сервере, время запуска назначается в назначенных заданиях. Программа будет осуществлять дозвон до удаленных серверов на которых будет поднят RRAS сервер и будет скачивать файлы с содержимым журналов – Application, Security, System, Dns.

На удаленном сервере должен быть открыт общий доступ к папке где хранится файл:  
- eventlog.rar

Все данные к программе задаются в файле [in.dat](#), который должен лежать строго в каталоге с программой, каждая строка в файле это отдельный сервер, данные вводятся через пробел. Какие данные используются – имя пользователя, пароль, телефон, имя домена, сетевой путь, число попыток дозвона.

Например

```
User1 123 p2110311 domen1 192.168.20.1\\c 6  
User2 145 p2110312 domen2 192.168.20.1\\b 8  
User3 156 p2110313 domen3 192.168.20.1\\a 7
```

User1	имя пользователя(созданный Active Directory)
123	пароль
p2110311	телефон
domen1	домен

192.168.0.20.1\\c	сетевой путь, где лежат файлы: - application.evlog - dns.evlog - security.evlog - system.evlog (этот сетевой путь соответствует <a href="#">\\192.168.0.20\\c\.</a> Например сетевой путь <a href="#">\\192.168.1.55\\a\\c\\b\</a> - 192.168.1.55\\a\\c\\b
6	число попыток

После скачивания файлов на диске С в каталоге temp, создается папка с номером цифры, где номер соответствует строке в файле in.dat.

### Тестируем запуск rras.exe

```

RemoteEvent - RrasDownload (Senkevich V.V. )

Server=1 Repetition=6
login - user
passwd - 123
telefon - p2110310
domen - domen
share - 192.168.20.1\\temp\\evlog
Connect
Download - eventlog.rar - 103Kb
eventlog.rar - OK
Connect razorvan

```

**Server=1** – в данный момент осуществляется работа с первым сервером, что соответствует первой строчке в файле in.dat

**Repetition=4** – этому серверу назначено 4 попытки дозвона

**login – user**

**passwd – 123**

Все эти данные были рассмотрены выше

**telefon – p129**

**domen – domen**

**share – 192.168.20.1\\temp\\evlog**

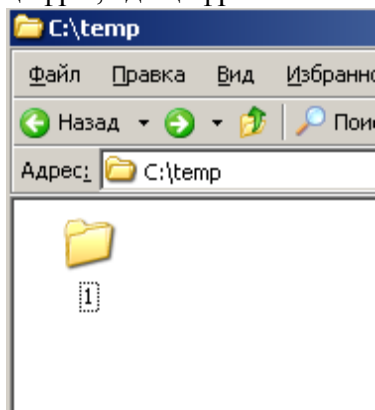
**Connect** – означает что соединение с удаленным сервером прошло успешно, если (**Connect no** – то соединение с сервером потерпело не удачу, соответственно дальше будет пытаться дозвониться еще, если назначены попытки в противном случае перейдет к следующему серверу.)

**eventlog.rar – OK**

Скаченный файл (при плохой связи файл будет пропущен)

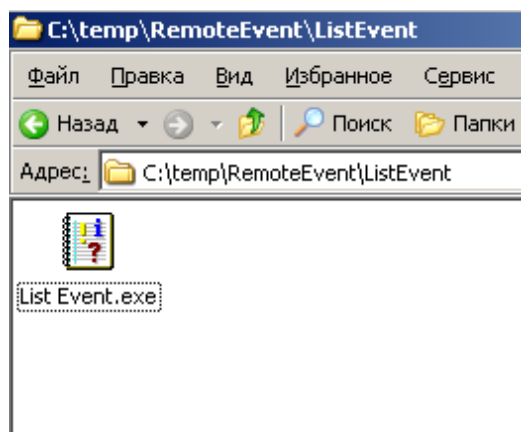
**Connect razorvan** – соединение с удаленным сервером разорвано, дальше автоматом будет осуществлен переход к следующему серверу.

После каждого разрыва соединения на диске С в каталоге temp, будет создана папка с номером цифры, где цифра соответствует параметру **Server=1**



### 3. ListEvent

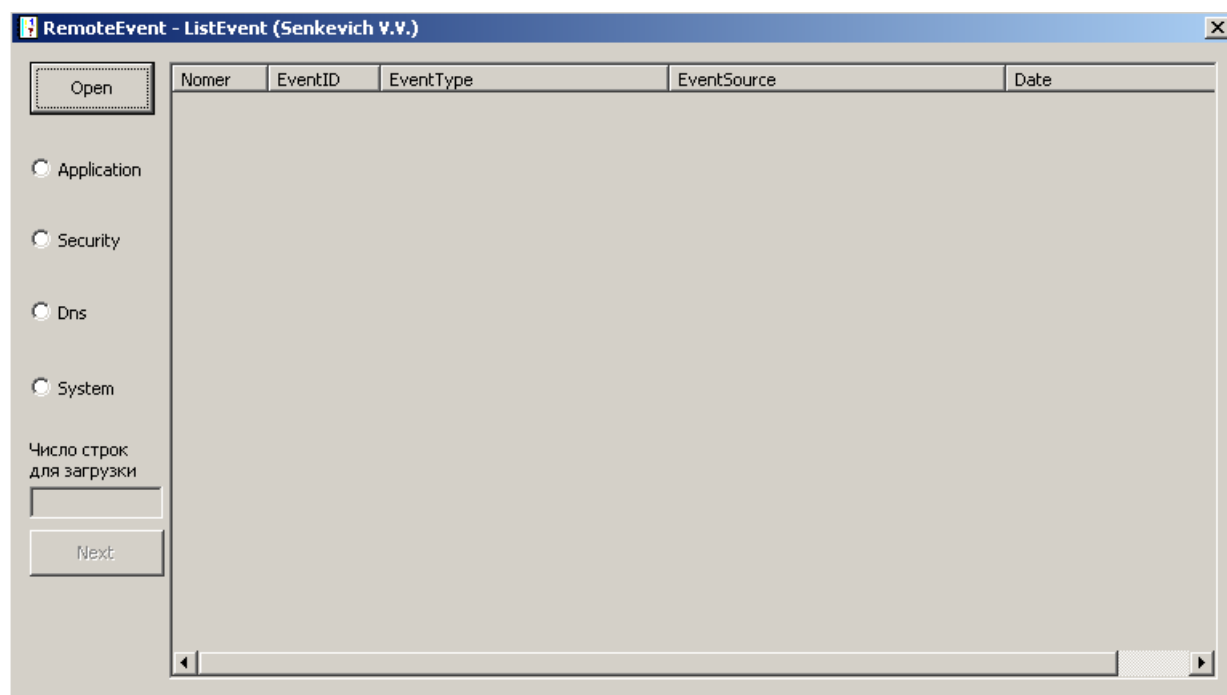
Внутри папки находится программа [List Event.exe](#).



Программа анализатор файлов

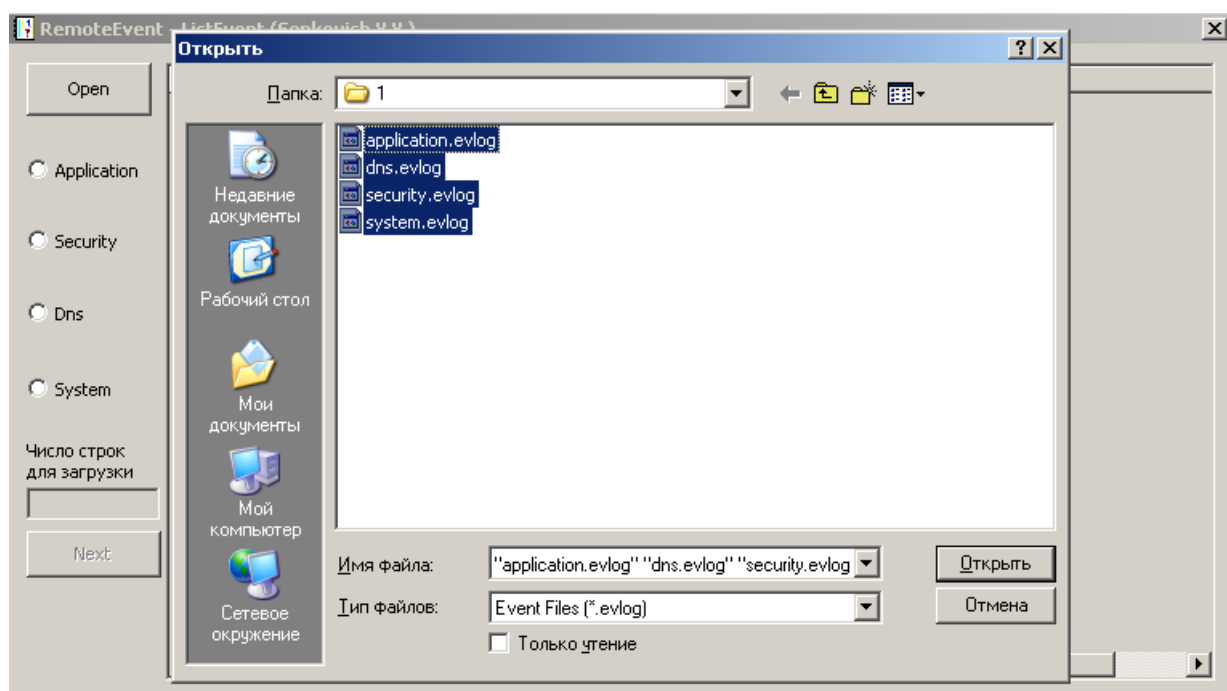
- application.evlog
- dns.evlog
- security.evlog
- system.evlog

**Тестируем запуск List Event.exe**



Нажимаем кнопку “Open” и выбираем файлы

- application.evlog
- dns.evlog
- security.evlog
- system.evlog




Переключение между журналами с помощью кнопок.

RemoteEvent - ListEvent (Senkevich V.V.)					
Open	Nomer	EventID	EventType	EventSource	Date
<input checked="" type="radio"/> Application	2083	781	EVENTLOG_INFORMATION_TYPE	COM+	5/25/2007 9:21:20
	2082	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:18
	2081	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:18
	2080	1003	EVENTLOG_INFORMATION_TYPE	Microsoft Search	5/25/2007 9:21:17
	2079	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:16
	2078	1000	EVENTLOG_INFORMATION_TYPE	VMware NAT Service	5/25/2007 9:21:15
	2077	1	EVENTLOG_INFORMATION_TYPE	VMware Virtual Mount Service Extended	5/25/2007 9:21:15
	2076	1000	EVENTLOG_INFORMATION_TYPE	VMware NAT Service	5/25/2007 9:21:14
	2075	9688	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2074	9666	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
<input type="radio"/> Security	2073	9666	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2072	3408	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2071	17137	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:12
	2070	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:12
	2069	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:12
	2068	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2067	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2066	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2065	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2064	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
<input type="radio"/> Dns	2063	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:9
	2062	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:9
	2061	17136	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2060	3454	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2059	3407	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2058	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2057	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2056	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2055	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2054	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
<input type="radio"/> System	2053	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:9
	2052	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:9
	2051	17136	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2050	3454	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2049	3407	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2048	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2047	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2046	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2045	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2044	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10

Нажимаете на событие и получаете соответственно его описание

RemoteEvent - ListEvent (Senkevich V.V.)					
Open	Nomer	EventID	EventType	EventSource	Date
<input checked="" type="radio"/> Application	2083	781	EVENTLOG_INFORMATION_TYPE	COM+	5/25/2007 9:21:20
	2082	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:18
	2081	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:18
	2080	1003	EVENTLOG_INFORMATION_TYPE	Microsoft Search	5/25/2007 9:21:17
	2079	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:16
	2078	1000	EVENTLOG_INFORMATION_TYPE	VMware NAT Service	5/25/2007 9:21:15
	2077	1	EVENTLOG_INFORMATION_TYPE	VMware Virtual Mount Service Extended	5/25/2007 9:21:15
	2076	1000	EVENTLOG_INFORMATION_TYPE	VMware NAT Service	5/25/2007 9:21:14
	2075	9688	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2074	9666	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
<input type="radio"/> Security	2073	9666	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2072	3408	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:14
	2071	17137	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:12
	2070	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:12
	2069	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:12
	2068	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2067	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2066	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2065	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2064	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
<input type="radio"/> Dns	2063	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:9
	2062	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:9
	2061	17136	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2060	3454	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2059	3407	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2058	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2057	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2056	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2055	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2054	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
<input type="radio"/> System	2053	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:9
	2052	1	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER/MSDE	5/25/2007 9:21:9
	2051	17136	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2050	3454	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2049	3407	EVENTLOG_INFORMATION_TYPE	MSSQL\$SQLEXPRESS	5/25/2007 9:21:6
	2048	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2047	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2046	17055	EVENTLOG_INFORMATION_TYPE	MSSQLSERVER	5/25/2007 9:21:11
	2045	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10
	2044	17055	EVENTLOG_INFORMATION_TYPE	MSSQL\$ADMIN	5/25/2007 9:21:10



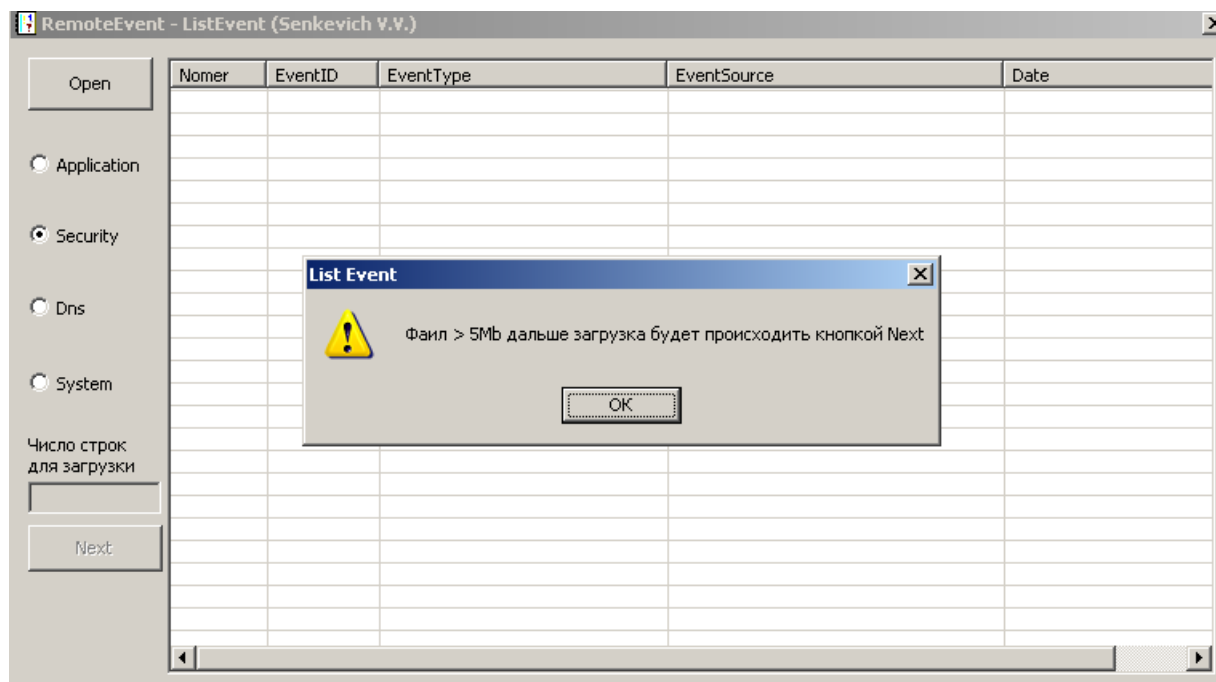
List Event

Подсистема COM+ подавляет повторяющиеся элементы журнала событий в течение 86400 сек. Таймаут подавления управляется значением REG\_DWORD с именем SuppressDuplicateDuration в следующем разделе реестра: HKLM\Software\Microsoft\COM3\Eventlog.

OK



Если какой нибудь из файлов превышает 5MB, то появиться соответственное сообщение и будет активирована кнопка “Next” и поле ввода “Число строк для загрузки”



В поле “Число строк для загрузки”, надо вводить число равное количеству строк, которое вы хотите подгрузить в программу и нажать кнопку “Next”

- Это нужно для того, чтобы программа не повисла при большом количестве информации

