



**СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВНОЕ УПРАВЛЕНИЕ КРИМИНАЛИСТИКИ
(КРИМИНАЛИСТИЧЕСКИЙ ЦЕНТР)**

**Криминалистический анализ исполнимых файлов
при помощи общедоступного программного обеспечения**

Докладчик: старший эксперт УОЭЖД
ГУК (КЦ) СК России
Вавилин А.Ю.

Москва
2019

Основные способы исследования исполнимых файлов

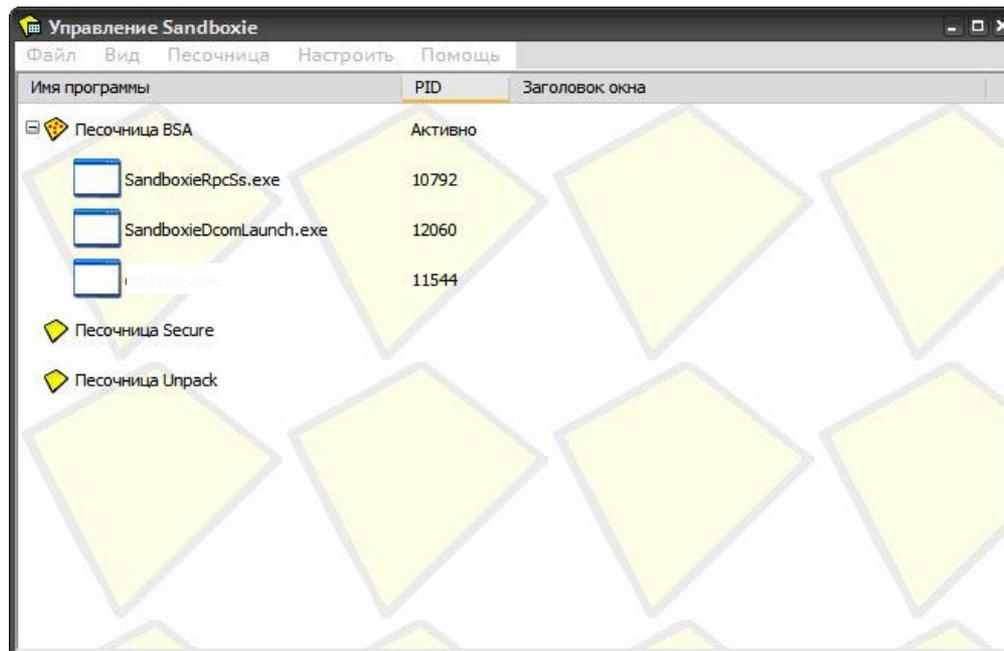
- *Виртуальные машины*



- *«Песочница» (Sandbox)*

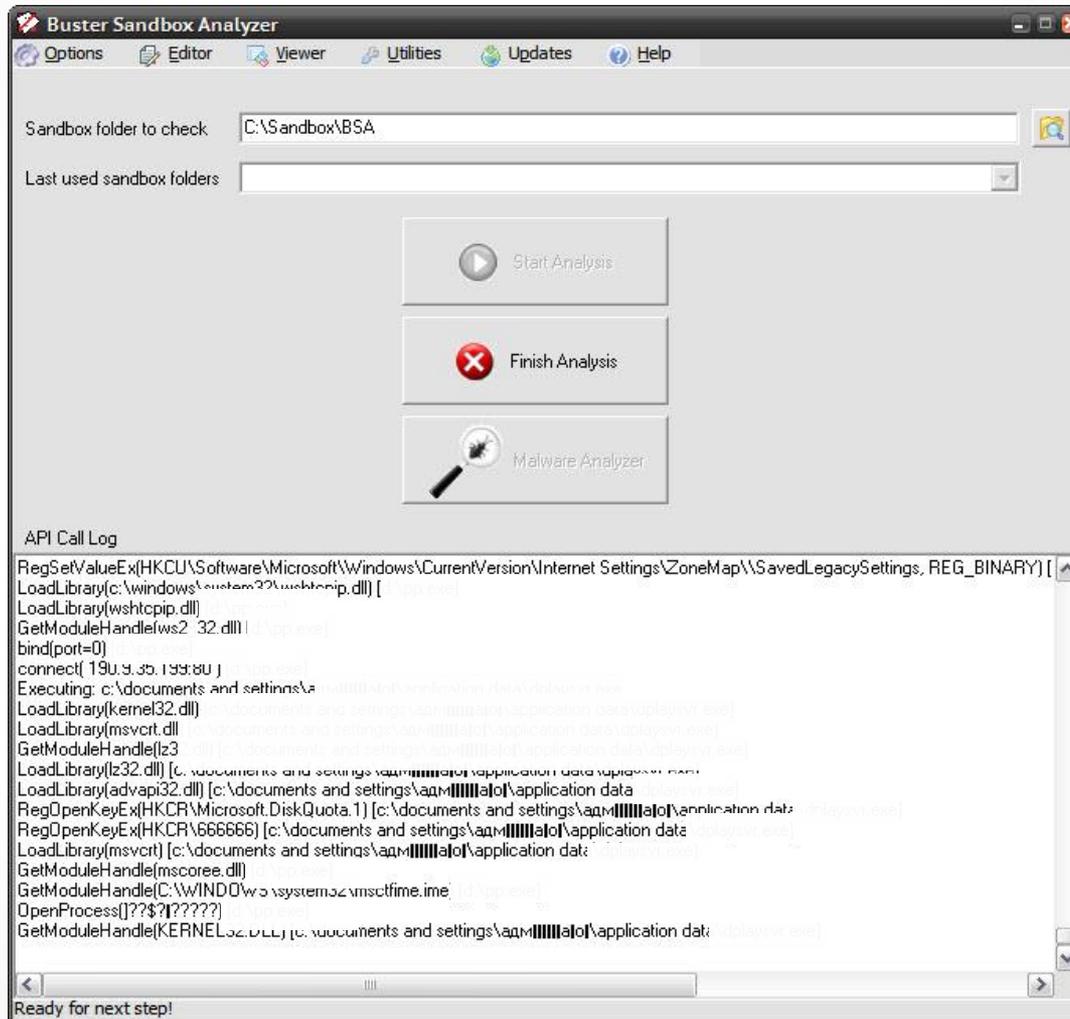


Использование «Песочницы» (Sandbox): «Sandboxie» + «Buster Sandbox Analyzer»



1. **Buster Sandbox Analyzer**
2. **SBIExtra** (обзор исполняемых процессов и потоков и др.)
3. **Antidel** (перехватывает функции, отвечающие за удаление файлов)

«Buster Sandbox Analyzer»



Использование «Песочницы» (Sandbox): «Sandboxie» + «Buster Sandbox Analyzer»

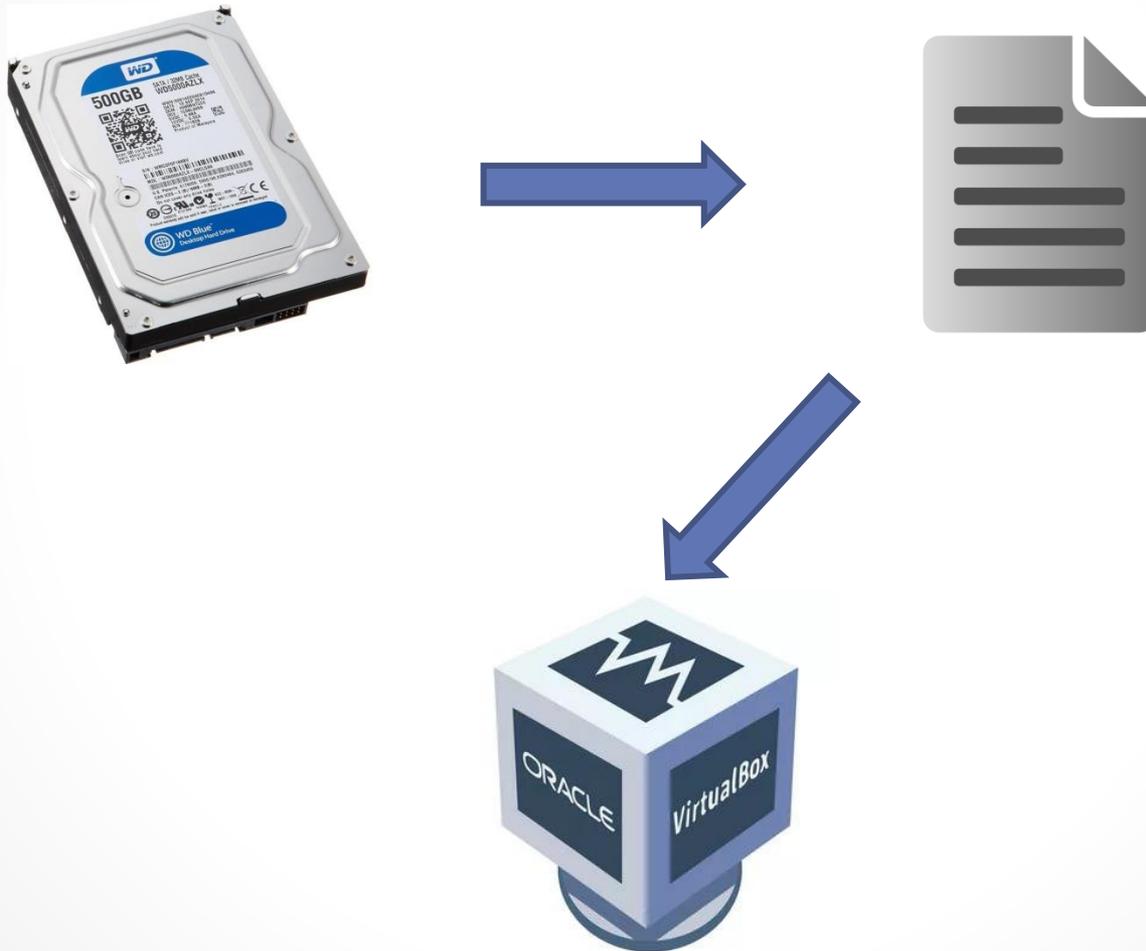


- Отслеживание API-вызовы запущенного приложения.
- Отслеживание создаваемых файлов и параметров реестра.
- Перехват сетевого трафика.
- Базовый анализ файлов и их поведения (встроенный поведенческий анализатор, анализ на VirusTotal по хешам, анализ с помощью PEiD, ExeInfo и ssdeep и т. д.).
- Получение дополнительной информации за счет выполнения в «песочнице» вспомогательных программ и др.



- Невозможен анализ файлов, выполняющихся в «kernel mode» (только на уровне «user mode»).
- Невозможен анализ файлов, отслеживающих выполнение в «Sandboxie» (в «Buster Sandbox Analyzer» имеются ряд механизмов, препятствующих такому отслеживанию).

Использование виртуальной машины и специального программного обеспечения

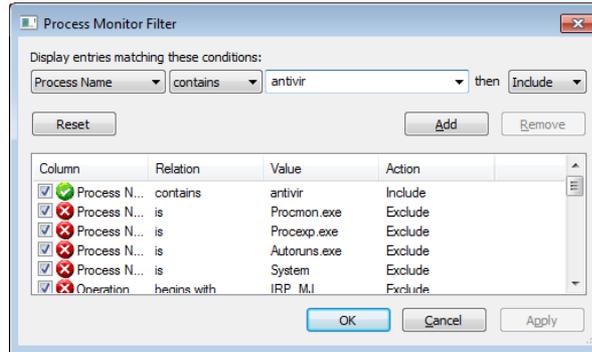


«Process Monitor»

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:27:...	SearchIndexer....	844	File System Control C:		SUCCESS	Control: FSCTL_R...
16:27:...	SearchIndexer....	844	File System Control C:		SUCCESS	Control: FSCTL_R...
16:27:...	Explorer.EXE	1472	Query Name Info...	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Name: \Users\Exp...
16:27:...	Explorer.EXE	1472	Create File	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Basic Infor...	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Creation Time: 19.0...
16:27:...	Explorer.EXE	1472	Close File	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users	SUCCESS	Filter: Users, 1: Users
16:27:...	Explorer.EXE	1472	Close File	C:\	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\Users	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users\Expert	SUCCESS	Filter: Expert, 1: Ex...
16:27:...	Explorer.EXE	1472	Close File	C:\Users	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\Users\Expert	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users\Expert\Desktop	SUCCESS	Filter: Desktop, 1: ...
16:27:...	Explorer.EXE	1472	Close File	C:\Users\Expert	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\Users\Expert\Desktop	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Filter: Procmon.exe...
16:27:...	Explorer.EXE	1472	Close File	C:\Users\Expert\Desktop	SUCCESS	
16:27:...	Explorer.EXE	1472	Query Name Info...	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Name: \Users\Exp...
16:27:...	Explorer.EXE	1472	Create File	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Basic Infor...	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	Creation Time: 19.0...
16:27:...	Explorer.EXE	1472	Close File	C:\Users\Expert\Desktop\Procmon.exe	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users	SUCCESS	Filter: Users, 1: Users
16:27:...	Explorer.EXE	1472	Close File	C:\	SUCCESS	
16:27:...	Explorer.EXE	1472	Create File	C:\Users	SUCCESS	Desired Access: R...
16:27:...	Explorer.EXE	1472	Query Directory	C:\Users\Expert	SUCCESS	Filter: Expert, 1: Ex...

Showing 442 444 of 653 438 events (67%) Backed by virtual memory

«Process Monitor»



16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 608 192, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 624 576, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 640 960, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 657 344, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 673 728, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 690 112, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 706 496, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 722 880, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 739 264, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 755 648, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 772 032, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 788 416, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 804 800, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 821 184, Length: 16 38
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 1 837 568, Length: 8 192
16:35:...	antivir.exe	3740	ReadFile	C:\Users\Expert\Desktop\files\1111y\Login\ant...	SUCCESS	Offset: 136 192, Length: 4 096, I
16:35:...	antivir.exe	3740	ReadFile	C:\Windows\winsxs\x86_microsoft.windows.co...	SUCCESS	Offset: 201 728, Length: 32 768
16:35:...	antivir.exe	3740	ReadFile	C:\Windows\winsxs\x86_microsoft.windows.co...	SUCCESS	Offset: 168 960, Length: 32 768
16:35:...	antivir.exe	3740	ReadFile	C:\Windows\winsxs\x86_microsoft.windows.co...	SUCCESS	Offset: 103 424, Length: 32 768
16:35:...	antivir.exe	3740	CreateFile	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	Desired Access: Generic Read, I
16:35:...	antivir.exe	3740	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefault.nls	FILE LOCKED WITH ...	Sync Type: SyncTypeCreateSecti
16:35:...	antivir.exe	3740	QueryStandardI...	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	AllocationSize: 2 945 024, EndOf
16:35:...	antivir.exe	3740	CreateFileMapp...	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	Sync Type: SyncTypeOther
16:35:...	antivir.exe	3740	CloseFile	C:\Windows\Globalization\Sorting\SortDefault.nls	SUCCESS	
16:35:...	antivir.exe	3740	CreateFile	C:\Windows\FonTS\sserifer fon	SUCCESS	Desired Access: Generic Read/E
16:35:...	antivir.exe	3740	QueryStandardI...	C:\Windows\FonTS\sserifer fon	SUCCESS	AllocationSize: 69 632, EndOfFile
16:35:...	antivir.exe	3740	QueryBasicInfor...	C:\Windows\FonTS\sserifer fon	SUCCESS	CreationTime: 13.07.2009 23:31:0
16:35:...	antivir.exe	3740	QueryAttributel...	C:\Windows\FonTS\sserifer fon	SUCCESS	FileSystemAttributes: Case Preser
16:35:...	antivir.exe	3740	CreateFileMapp...	C:\Windows\FonTS\sserifer fon	FILE LOCKED WITH ...	Sync Type: SyncTypeCreateSecti
16:35:...	antivir.exe	3740	QueryStandardI...	C:\Windows\FonTS\sserifer fon	SUCCESS	AllocationSize: 69 632, EndOfFile
16:35:...	antivir.exe	3740	CreateFileMapp...	C:\Windows\FonTS\sserifer fon	SUCCESS	Sync Type: SyncTypeOther
16:35:...	antivir.exe	3740	CloseFile	C:\Windows\FonTS\sserifer fon	SUCCESS	
16:35:...	antivir.exe	3740	CreateFile	C:\Users\Expert\Desktop\files\1111y\Login	SUCCESS	Desired Access: Read Data/List
16:35:...	antivir.exe	3740	QueryDirectory	C:\Users\Expert\Desktop\files\1111y\Login\11	NO SUCH FILE	Filter: 11
16:35:...	antivir.exe	3740	CloseFile	C:\Users\Expert\Desktop\files\1111y\Login	SUCCESS	

СПАСИБО ЗА ВНИМАНИЕ!