СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЛАВНОЕ УПРАВЛЕНИЕ КРИМИНАЛИСТИКИ
(КРИМИНАЛИСТИЧЕСКИЙ ЦЕНТР)

Криминалистический анализ исполнимых файлов при помощи общедоступного программного обеспечения

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

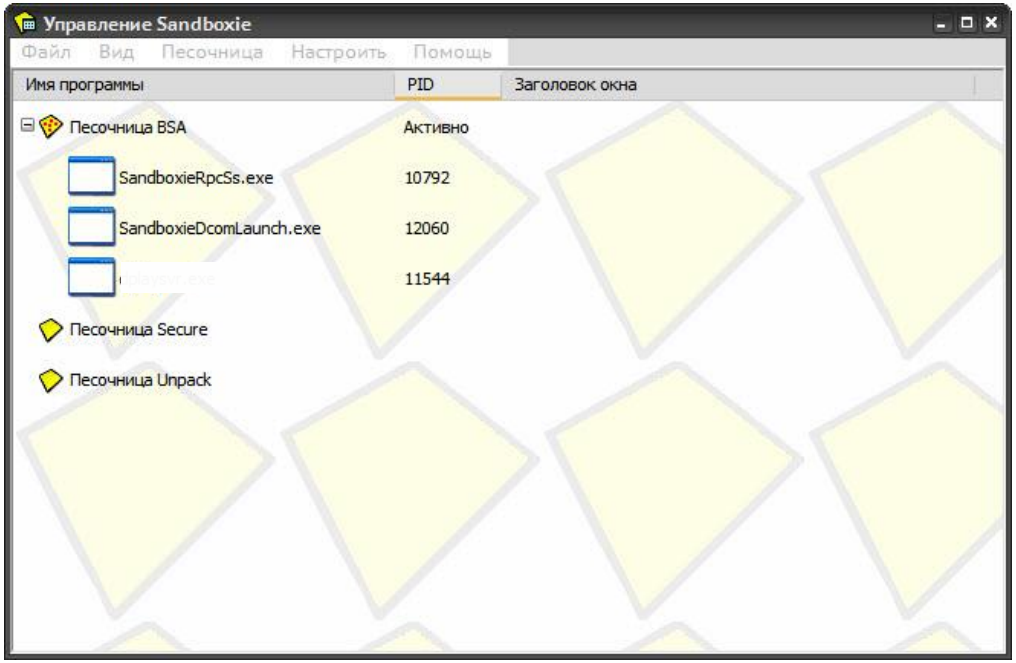
Москва
2019

Основные способы исследования исполнимых файлов

- Виртуальные машины

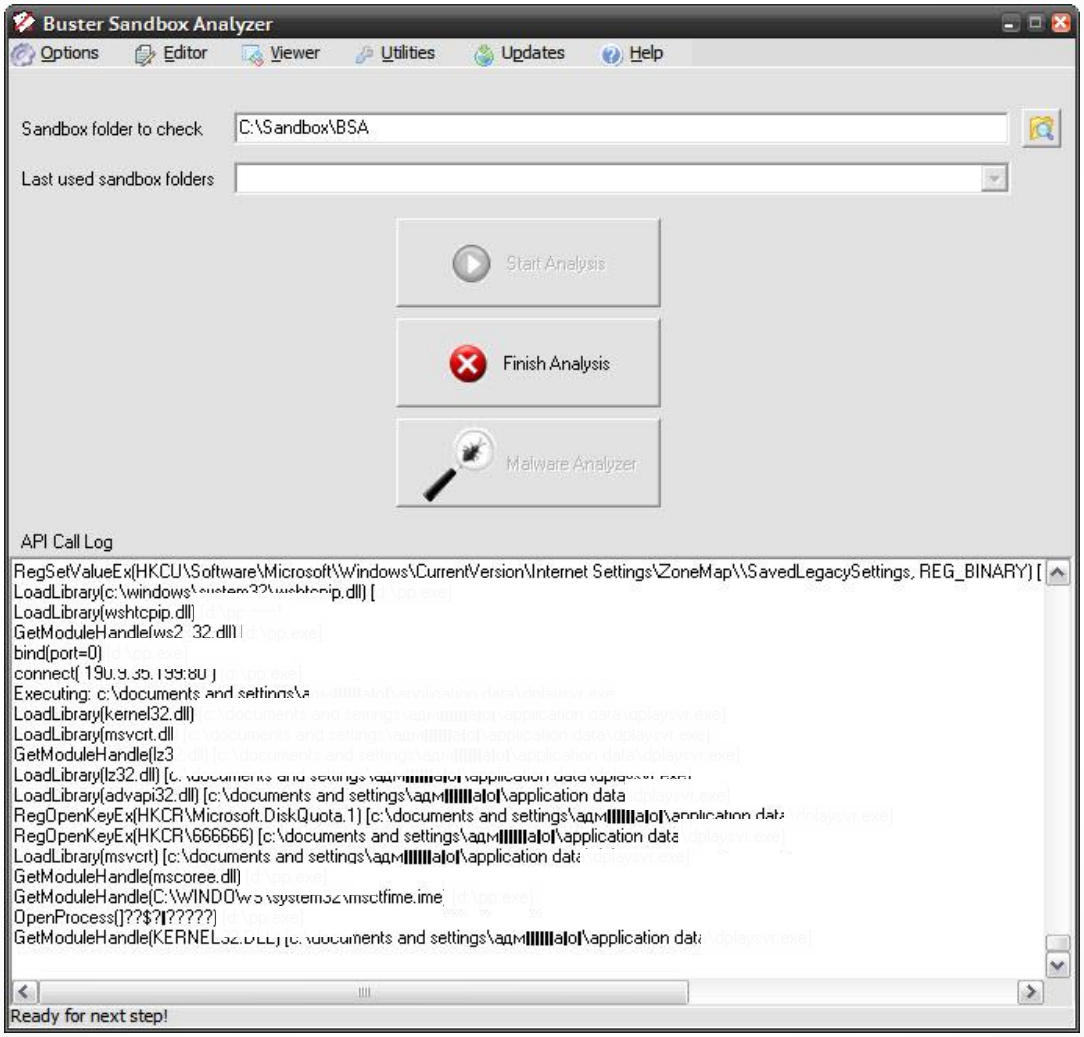
- «Песочница» (Sandbox)

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»



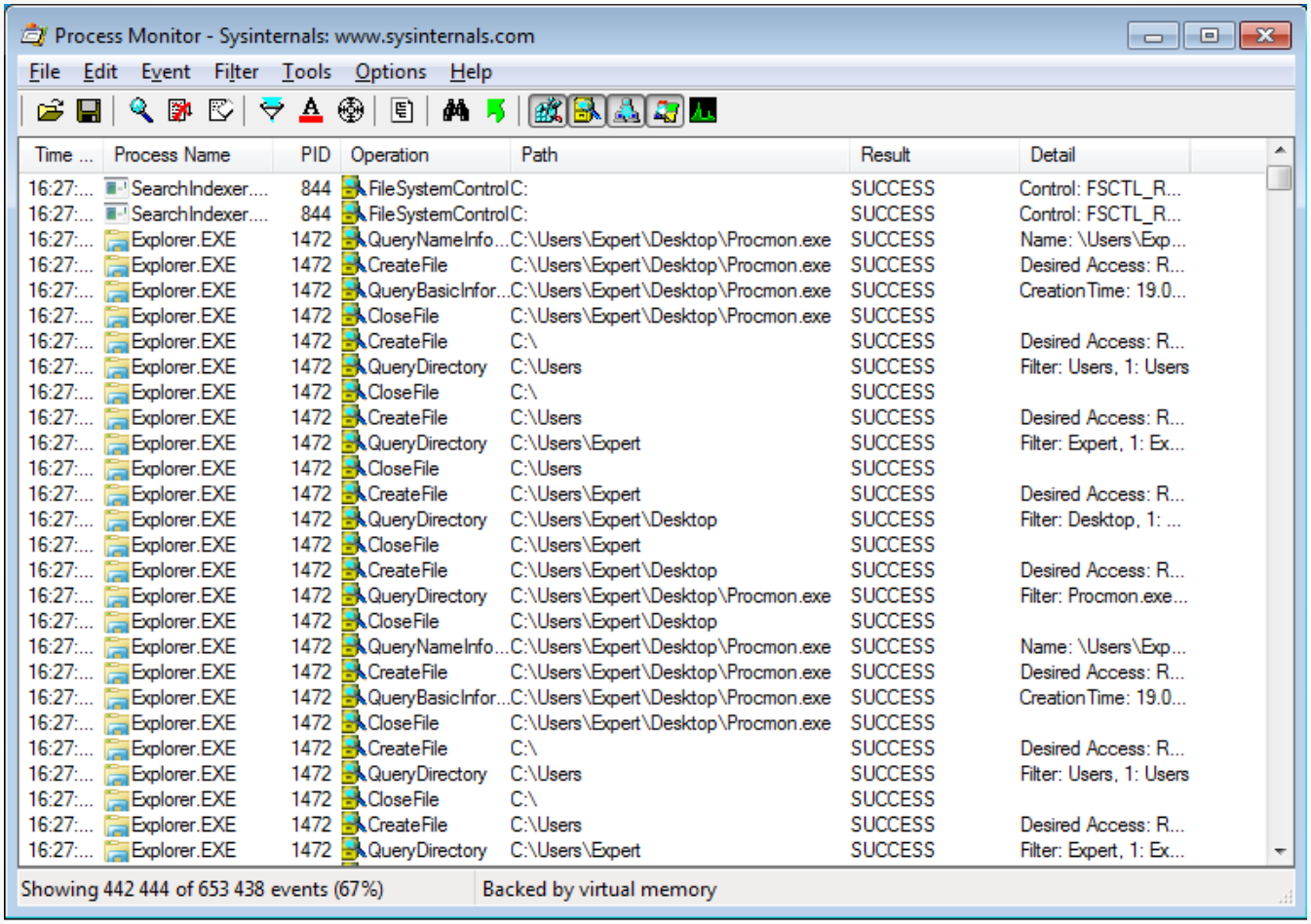
Использование «Песочницы» (Sandbox): «Sandboxie» + «Buster Sandbox Analyzer»

- 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.

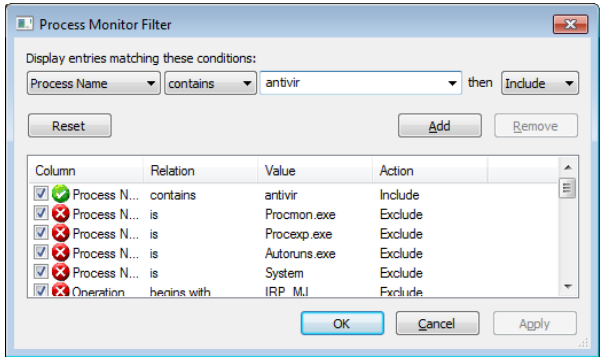
- Невозможен анализ файлов, выполняющихся в «kernel mode» (только на уровне «user mode»).
- Невозможен анализ файлов, отслеживающих выполнение в «Sandboxie» (в «Buster Sandbox Analyzer» имеются ряд механизмов, препятствующих такому отслеживанию).

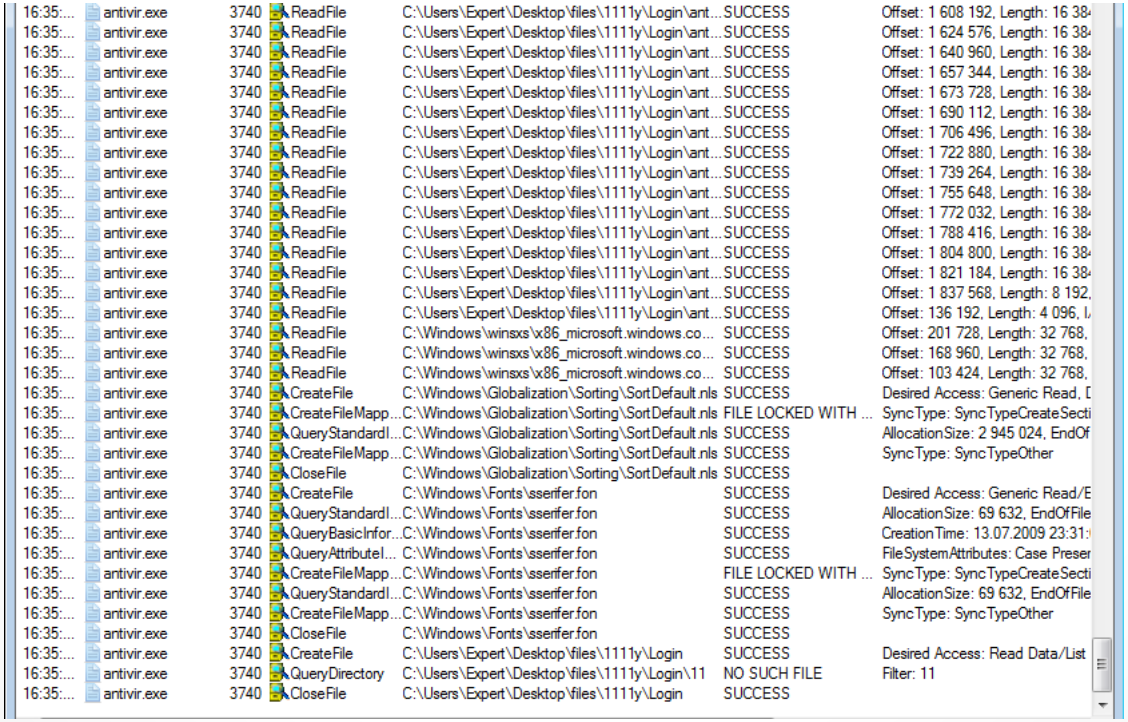
Использование виртуальной машины и специального программного обеспечения

«Process Monitor»



«Process Monitor»





СПАСИБО ЗА ВНИМАНИЕ!