Компьютерная криминалистика в корпоративных расследованиях

Акулов Александр Александрович
akulov@in4security.com

softline®

Учебный центр

Объекты компьютерно-технической экспертизы

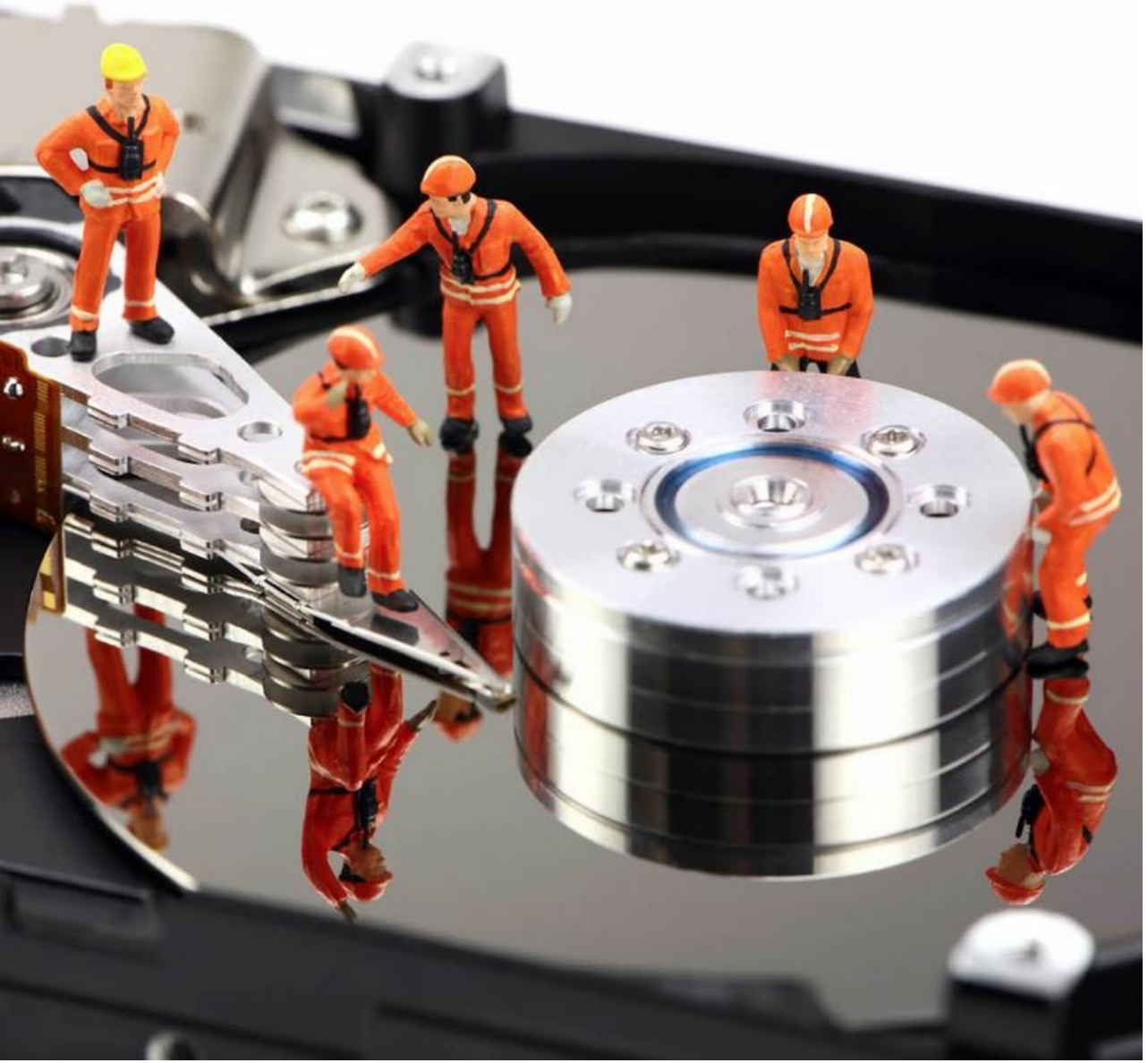
Аппаратные

Информационные

Программные

Сетевые

Получение копии цифрового доказательства



Цифровые объекты как улики

Все манипуляции осуществляются **только над копией** носителя!

Оригинал остается **нетронутым!**

Кто может быть экспертом?

Федеральный закон от 31 мая 2001 г. N 73-ФЗ "О государственной судебно-экспертной деятельности в Российской Федерации" (с изменениями и дополнениями)

Глава VI. Заключительные положения

Федеральным законом от 25 ноября 2013 г. N 317-ФЗ в статью 41 настоящего Федерального закона внесены изменения
См. текст статьи в предыдущей редакции

Статья 41. Распространение действия настоящего Федерального закона на судебно-экспертную деятельность лиц, не являющихся государственными судебными экспертами

См. комментарии к статье 41 настоящего Федерального закона

В соответствии с нормами процессуального законодательства Российской Федерации судебная экспертиза может производиться вне государственных судебно-экспертных учреждений лицами, обладающими специальными знаниями в области науки, техники, искусства или ремесла, но не являющимися государственными судебными экспертами.

На судебно-экспертную деятельность лиц, указанных в части первой настоящей статьи, распространяется действие статей 2, 3, 4, 6 - 8, 16 и 17, части второй статьи 18, статей 24 и 25 настоящего Федерального закона.

Статья 42. Приведение нормативных правовых актов в соответствие с настоящим Федеральным законом

См. комментарии к статье 42 настоящего Федерального закона

Поручить Правительству Российской Федерации обеспечить приведение нормативных правовых актов федеральных органов исполнительной власти в соответствие с настоящим Федеральным законом.

Статья 43. Вступление в силу настоящего Федерального закона

См. комментарии к статье 43 настоящего Федерального закона

Настоящий Федеральный закон вступает в силу со дня его официального опубликования, за исключением части третьей статьи 29, которая вступает в силу после приведения уголовно-процессуального законодательства Российской Федерации в соответствие с положениями Конституции Российской Федерации.

Президент Российской Федерации В. Путин

softline®

Учебный центр

Основания для отвода эксперта:

- Некомпетентность эксперта
- Личная заинтересованность в исходе дела
- Служебная или иная зависимость от лица, заинтересованного в исходе дела

Базовый состав мобильного рабочего места эксперта

- Ноутбук
- Переходник SATA/IDE – USB
- Дубликатор жестких дисков
- Набор кабелей и адаптеров
- Внешние накопители
- Комплект загрузочных дисков
- Набор инструментов
- Комплект для маркировки
- Удлинитель с сетевым фильтром
- Портативный источник питания
- Средства физической защиты
- Wi-Fi GSM роутер

Базовый состав ПО для лаборатории

- AccessData FTK (или EnCase, Belkasoft EC)
- Мобильный Криминалист (или UFED)
- dtSearch Desktop
- WinHex
- SysTools MailXaminer
- USB Block
- TrueCrypt
- NirSoft Utilities
- Volatility
- VirtualBox
- Elcomsoft Utilities

В моей выездной сумке

Работа с дубликатором Tableau TD2

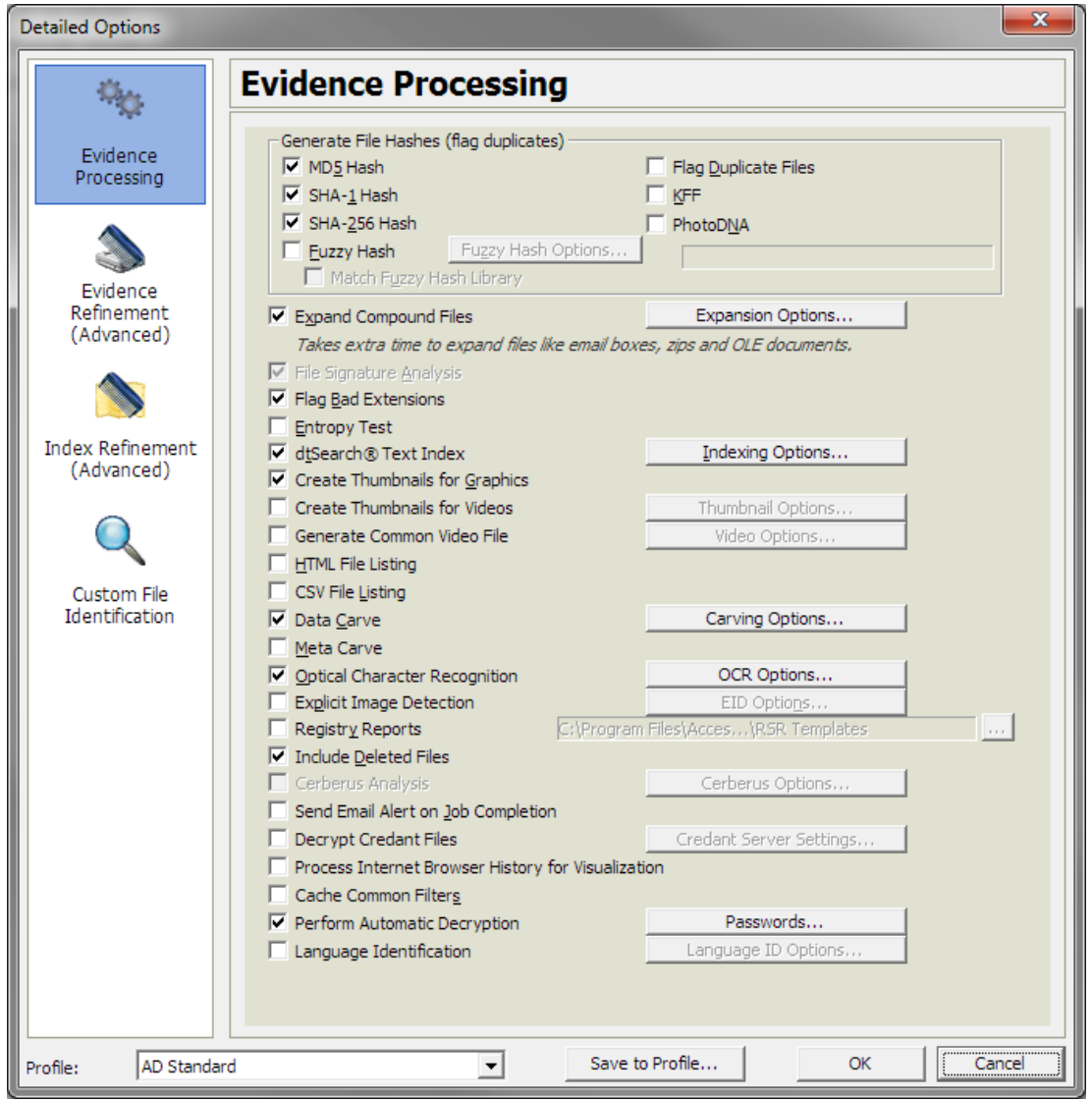
Источник

Копия 1

Копия 2

FireWire порт

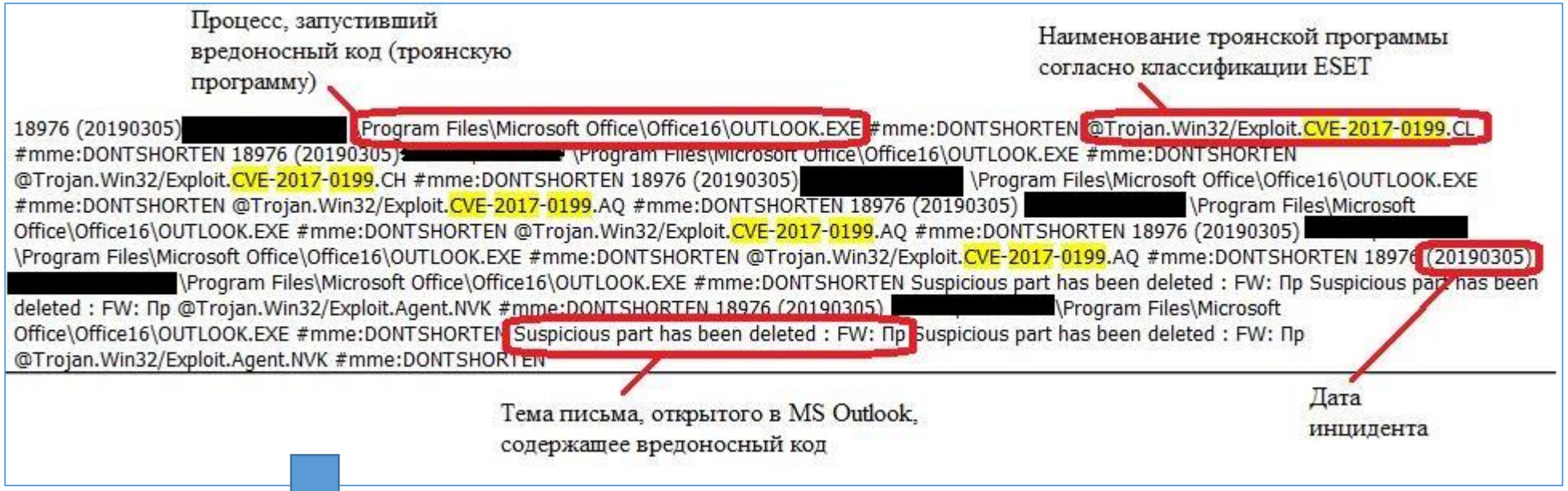
USB (2 порта)

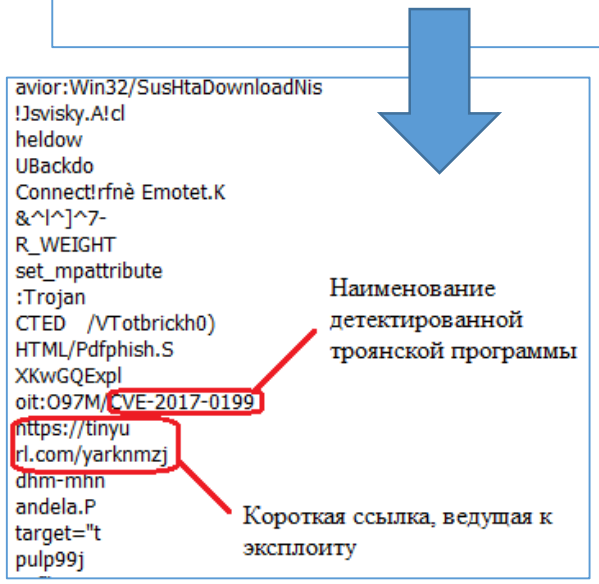


Машинный анализ. AccessData Forensic Toolkit.

- Expand Compound Files – обработка вложенных файлов внутри форматов 7z, RAR, MBOX, EXIF, кэш браузеров и др.
- dtSearch Text Index – автоматическое индексирование содержимого образа
- Data Carve – Восстановление удаленных данных с помощью поиска по сигнатурам
- Optical Character Recognition (OCR) – распознавание текста в графических файлах
- Perform Automatic Decryption – автоматическая дешифрация с помощью списка паролей

Пример





softline®

Учебный центр

Лаборатория компьютерной криминалистики Инфосекьюрити

INFOSECURITY

Чем занимаются

- Проведение судебной компьютерно-технической экспертизы, участие в процессуальных действиях в качестве специалистов, расследование инцидентов информационной безопасности.

Основные компетенции

- Всестороннее исследование компьютерной техники и цифровых носителей информации с помощью современных аппаратно-программных комплексов в интересах бизнеса и частных лиц.

Специалисты

- Специалисты Лаборатории компьютерной криминалистики Инфосекьюрити имеют профильную сертификацию и являются действительными членами Палаты судебных экспертов имени Ю.Г. Корухова.

softline®

Учебный центр

Акулов Александр Александрович
akulov@in4security.com

СПАСИБО ЗА ВНИМАНИЕ

ВОПРОСЫ?