Россия, 2018

ЭЛЕКТРОННЫЕ ДОКАЗАТЕЛЬСТВА

СЛУЧАЙ ИЗ ПРАКТИКИ - ГАРЛАСКО

ДОПУСТИМОСТЬ ДОКАЗАТЕЛЬСТВ

ДЕЛО ГАРЛАСКО

- Кьяра Поджи была убита 13 августа 2007 г.
  - Ее парень, Альберто Стази, провел с ней ночь перед убийством
  - Подозреваемый
- Решение суда первой инстанции - оправдательный приговор - декабрь 2009 г.
- Апелляционный суд – решение подтверждено - декабрь 2011 г.
- Верховный суд отменяет приговор и возвращает дело в Апелляционный суд – апрель 2013 г.
- Повторное рассмотрение дела - Альберто был приговорен к 16 годам лишения свободы и штрафу в размере 1 млн. евро - декабрь 2014 г.
- В чем важность данного дела?

ДЕЛО ГАРЛАСКО

- Его алиби: в момент убийства он был у себя дома, работая над дипломным проектом
- Добровольно отдал свой ноутбук полиции
- Сотрудники полиции, которые проверяли ноутбук, не были экспертами
- Цель полиции: установить действия, выполнявшиеся на ноутбуке

ДЕЛО ГАРЛАСКО

- Ноутбук включался 7 раз
- Вставлялось несколько USB-дисков
- Доступ к документам по Дипломному проекту
- У Альберто был доступ к ноутбуку во время проведения «проверки».

ДЕЛО ГАРЛАСКО

- Через некоторое время эксперты-криминалисты провели судебную экспертизу ноутбука
- Последствия «проверки»:
  - Произведен доступ к более чем 39 000 документов
  - Изменено более 500 файлов
  - Создано более 500 новых файлов
  - Изменены метаданные дипломного проекта

ДЕЛО ГАРЛАСКО

- Отсутствие системы охраны доказательств при их передаче
- Проверка подлинности и целостность цифровых доказательств нарушены
- Следователи не компетентны
- Отсутствует контрольный след

СЛУЧАЙ ИЗ ПРАКТИКИ - БЕНДИ

ДЕЛО БЕНДИ

- Компания Yahoo! отправила в Национальный центр поиска пропавших и эксплуатируемых детей CyberTipline отчет о непристойных фотографиях детей, загруженных на один из ее серверов - ноябрь 2004 г.
  - Фотографии были загружены 07 ноября 2004 г.
  - Фотографии загружены в группу Yahoo! „beth-lard9”
  - Ник пользователя, загрузившего фотографии - „mrbob1980hoopdu”
- В чем важность данного дела?

ДЕЛО БЕНДИ

- Yahoo! предоставила данные пользователя полиции
  - Полное имя: «Г-жа Джо Бин»
  - Город - Феникс
  - Штат - Аризона
  - Учетная запись «mrbob1980hoopdu» создана 05 ноября 2004 г.
  - IP-адрес 68.98.62.49 (Компания Cox Communications)

ДЕЛО БЕНДИ

- Полиция подтвердила, что учетная запись была зарегистрирована на Грега Бенди, 1425 E Десерт Брум Вей, Феникс
- Во время домашнего обыска Мэтью Бенди (сын Грега) сообщил полиции:
  - Он создал учетную запись «joebean1988hoopdu»
  - Он отрицал, что ему было что-либо известно об учетной записи „mrbob1980hoopdu”
  - Он заявил, что смотрел порнографию с участием взрослых
  - Он не загружал никаких изображений

ДЕЛО БЕНДИ

- Экспертно-криминалистический осмотр компьютера проводился детективом, сертифицированным Международной ассоциацией специалистов по компьютерным расследованиям (IACIS)
  - Используя текстовый поиск, он обнаружил:
    - Ник „mrbob1980hoopdu” упоминался 80 раз
    - Группа Yahoo! „beth_lard9” упоминалась 500 раз
    - Уменьшенные изображения непристойных фотографий детей также были найдены
  - Компьютер и CD были изъяты

ДЕЛО БЕНДИ

- Первая криминалистическая экспертиза, проведенная полицией
  - В одной папке найдено 72 порнографических изображения детей
  - С помощью текстового поиска было обнаружено:
    - Ник «mrbob1980hoopdu» упоминался 299 раз
    - Группа Yahoo! «beth_lard9» упоминалась 949 раз
    - В папке «Temporary Internet files» («Временные файлы Интернета») находились удаленные порнографические изображения взрослых
    - В папке «Recycler Folder» («Корзина») были изображения маленьких детей, файлы, содержащие ссылки на порнографию, удаленные различные порнографические файлы
    - Профиль пользователя «mrbob1980hoopdu» находился на жестком диске
    - Адрес электронной почты «mrbob992000» находился на жестком диске
    - В выделенных кластерах содержалась основная информация пользователя (Ereg), относящаяся к Мэтту Бенди, адрес электронной почты которого - «mrbob1980hoopdu@yahoo.com»

ДЕЛО БЕНДИ

- Первая криминалистическая экспертиза, проведенная полицией
  - Криминалистическая экспертиза изъятых CD-дисков
    - Найдена 51 папка, содержащая свыше 2800 непристойных фотографий детей, порнографических материалов со взрослыми и анимированную детскую порнографию
    - Папка с именем «kid \ lolita \ goodones» содержала непристойные фотографии детей
  - Бенди утверждал, что компакт-диск был резервной копией всей компьютерной системы
    - Это было невозможно, поскольку диск был емкостью 650 МБ, а компьютер содержал более 100 ГБ

ДЕЛО БЕНДИ

- Вторая криминалистическая экспертиза, проведенная полицией
  - ОС была установлена 09 апреля 2003 г. и переустановлена 04 декабря 2004 г.
  - Папка, содержавшая непристойные фотографии, была создана 04 декабря 2004 г.
  - Непристойные изображения находились на жестком диске и на компакт-диске
  - Хэш MD5 совпал на всех изображениях
  - Полиция утверждала, что вредоносный вирус, троян, червь или хакер не могли
    - создать ник «mrbob1980hoopdu» с информацией пользователя Мэтта Бенди
    - скачать файлы с детской порнографией 11 ноября 2004 г.
    - Записать непристойные изображения на CD
    - Переустановить ОС компьютера
    - Создать папку с именем «kid\lolita\goodones»

ДЕЛО БЕНДИ

- Криминалистическая экспертиза в интересах защиты
  - Следователь указал на более 200 зараженных файлов на компьютере
  - Одна или несколько вредоносных программ, обнаруженных в системе, переименовали значительное количество компьютерных файлов, что делает невозможным обнаружение всех операций
  - Все действия на этом компьютере выполнялись под стандартной учетной записью пользователя «Владелец»
  - Антивирус и брандмауэр на системе были отключены
  - В системе были обнаружены следующие атаки:
    - Backdoor.W32.Rbot
    - Backdoor.W32.gen
    - TrojanProxy.Win32.Bobax.c
    - Win32.Winshow.G
    - Divx.exe
    - Instsrv.exe

ДЕЛО БЕНДИ

- Третья криминалистическая экспертиза, проведенная полицией
  - Следствие выявило только две вредоносные программы на жестком диске
  - Вирус instsrv.exe являлся рекламной программой, которая не может удаленно управлять компьютером
  - Вирус divx.exe был создан для того, чтобы целевые пользователи, скачивающие детскую порнографию и незаконное программное обеспечение,получали сообщение «не удалось загрузить URL»

ДЕЛО БЕНДИ

- Вывод:
  - Члены коллегии присяжных не имеют обширных знаний в области компьютерной криминалистики
  - Судья также не обладает знаниями в компьютерной криминалистике и, как правило, должен хорошо подготовиться к судебному разбирательству (должен прочитать большое количество статей)
  - Адвокаты обеих сторон пытаются «использовать» пробелы в образовании присяжных и судей
  - Адвокаты должны доказать, что они предприняли надлежащие шаги, чтобы ознакомиться с цифровыми доказательствами

ДЕЛО БЕНДИ

- Мэтт Бенди был условно осужден на 18 месяцев

Цифровые доказательства

- Любая информация, имеющая доказательную силу, переданная в запоминающее устройство или отправленная в цифровом формате

  - определение Научной рабочей группы по цифровым доказательствам (SWGDE - 1999)

- Данные, сгенерированные, сохраненные или передаваемые с использованием электронных устройств, которые можно использовать в суде.

  -- Совет Европы, 2013 г.

Мы не можем это ни увидеть, ни почувствовать, ни потрогать!

Цифровые доказательства и знания

- Кто что должен знать?
  - Адвокаты о цифровых доказательствах
  - Эксперты-криминалисты о законодательстве
- Характеристики цифровых доказательств
  - Легко уничтожаются, даже не оставляя об этом следов
  - Трудно спрятать, но и найти непросто.

Допустимость

- Рекомендации по проверке доказательств с целью обоснования их использования в судебных процедурах:

1. Надежность

   Являются ли доказательства надежными, не содержащими ошибок, и используются ли надлежащие процедуры?

2. Подлинность

   Откуда получены доказательства?

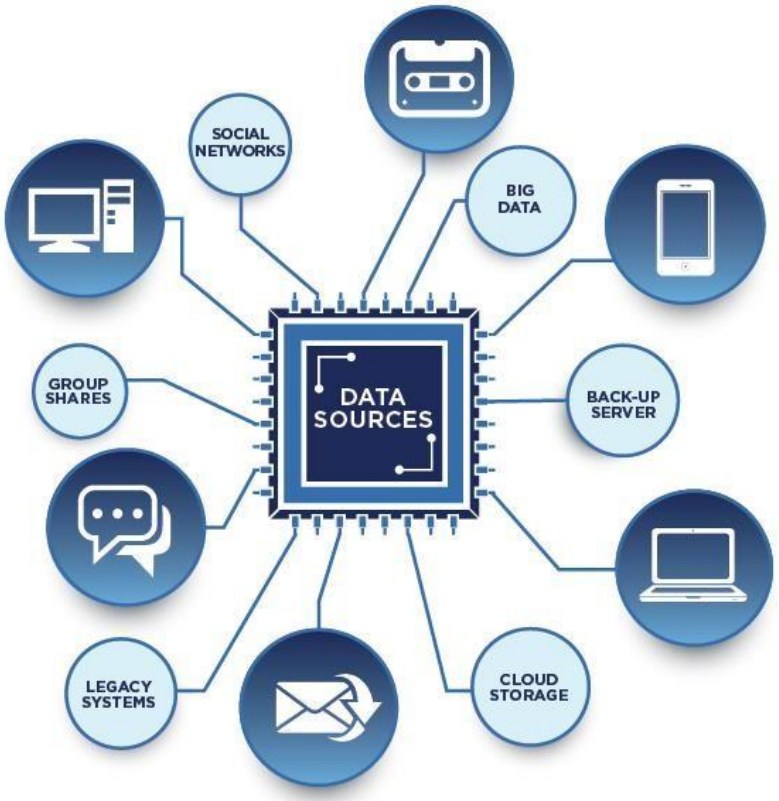
3. Полнота

   Все ли охвачены аспекты?

4. Правдоподобие

   Кажутся ли они понятными и правдоподобными присяжным?

Виды цифровых доказательств



- Хранимые данные
  - HDD, SSD, USB, CD…
- Не сохраняющиеся данные (из оперативной памяти)
- Данные мобильных устройств
- Сетевые данные
- Интернет-данные
- Данные в облаке

ДОКУМЕНТАЦИЯ

- **Начинается:**

когда следователя вызывают на место преступления

- **Заканчивается:**

в момент закрытия дела

Проблемы

Нематериальность

- Доказательства нельзя изучить физически

Анонимность

- Как жертв, так и правонарушителей

Непостоянство

- Неправильное хранение, скачки напряжения, заражение вредоносными программами, неправильный сбор данных

Удаление

- Можно восстановить
- Могут остаться копии в таких местах, о которых не знают

Нет дополнительных судебно-криминалистических улик

- Очевидцев, отпечатков пальцев, ДНК

Проблемы

Физическое распространение

- Доказательства могут быть разбросаны по всему миру
- Могут применяться местные, государственные, международные законы

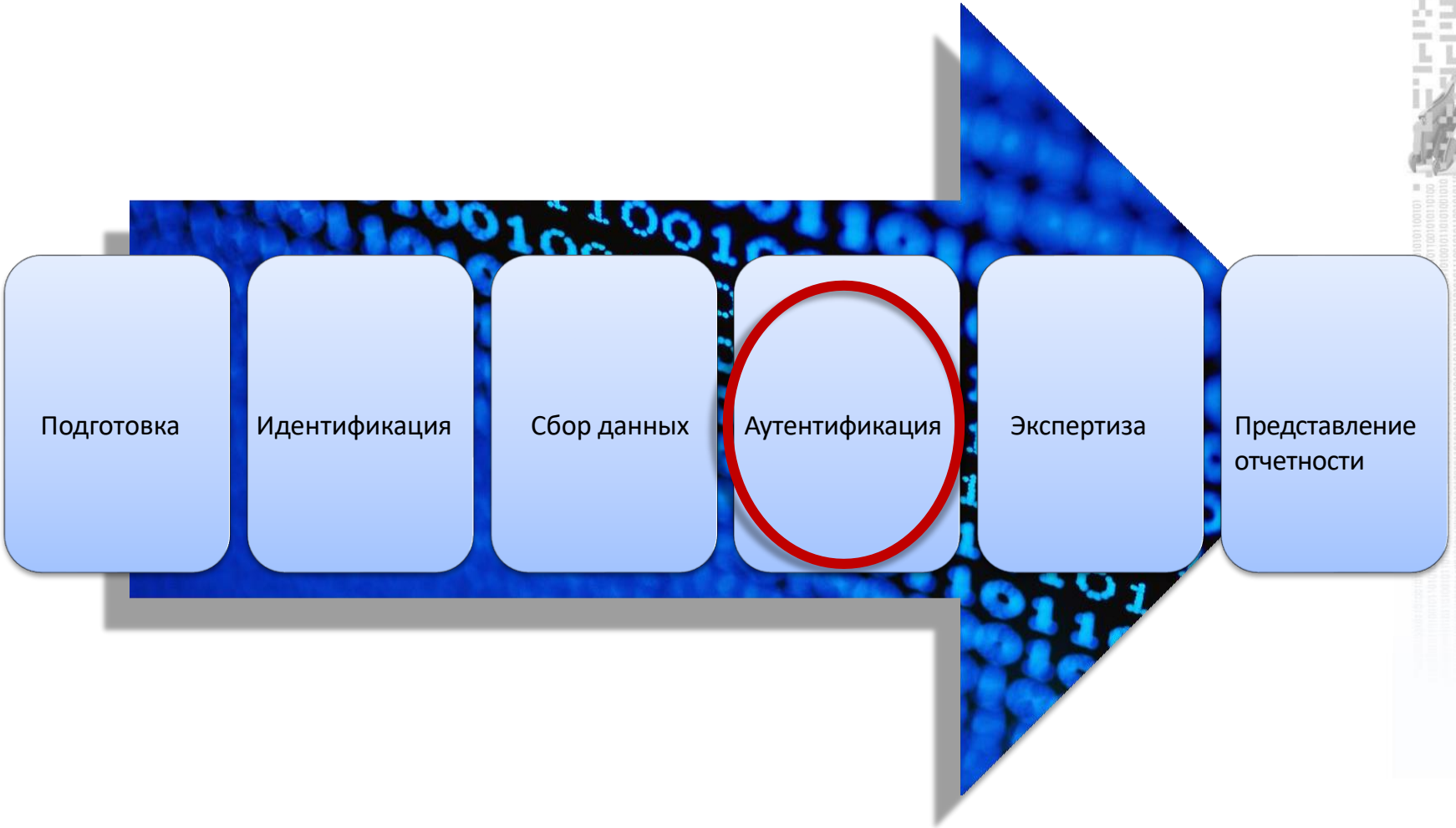
Скорость

- Взаимодействие становится более быстрым, недорогим и доступным

Легкий доступ к хакерским инструментам

Большой объем доступного пространства для хранения

Методология



Аутентификация

- Гарантия того, что данные, полученные с компьютера, являются точными дубликатами
- Сравнение данных, продублированных в процессе обработки изображений, с исходными данными на компьютере подозреваемого

Ведь если это не идеальный дубликат, как суд узнает, что все, что вы нашли, действительно было на исходном компьютере?

Почему мы заботимся о целостности?

- Принцип цифровой криминалистики
  - Расследование всегда ведется (если это возможно) на копии цифровых носителей
- Сохранение оригинала от уничтожения
- Обеспечение возможности повторного расследования
  - Защита желает повторить процедуру
  - Подтверждение выводов при помощи другого инструмента

Целостность цифровых доказательств

- Представляемые в суд доказательства должны быть полными и неизмененными
- несколько принятых научных методов для доказательства целостности:
  - Контрольная сумма
  - Алгоритмы хэширования
  - Цифровая подпись
  - Добавление метки времени
- Криминалистические инструменты по умолчанию обеспечивают применение некоторых методов

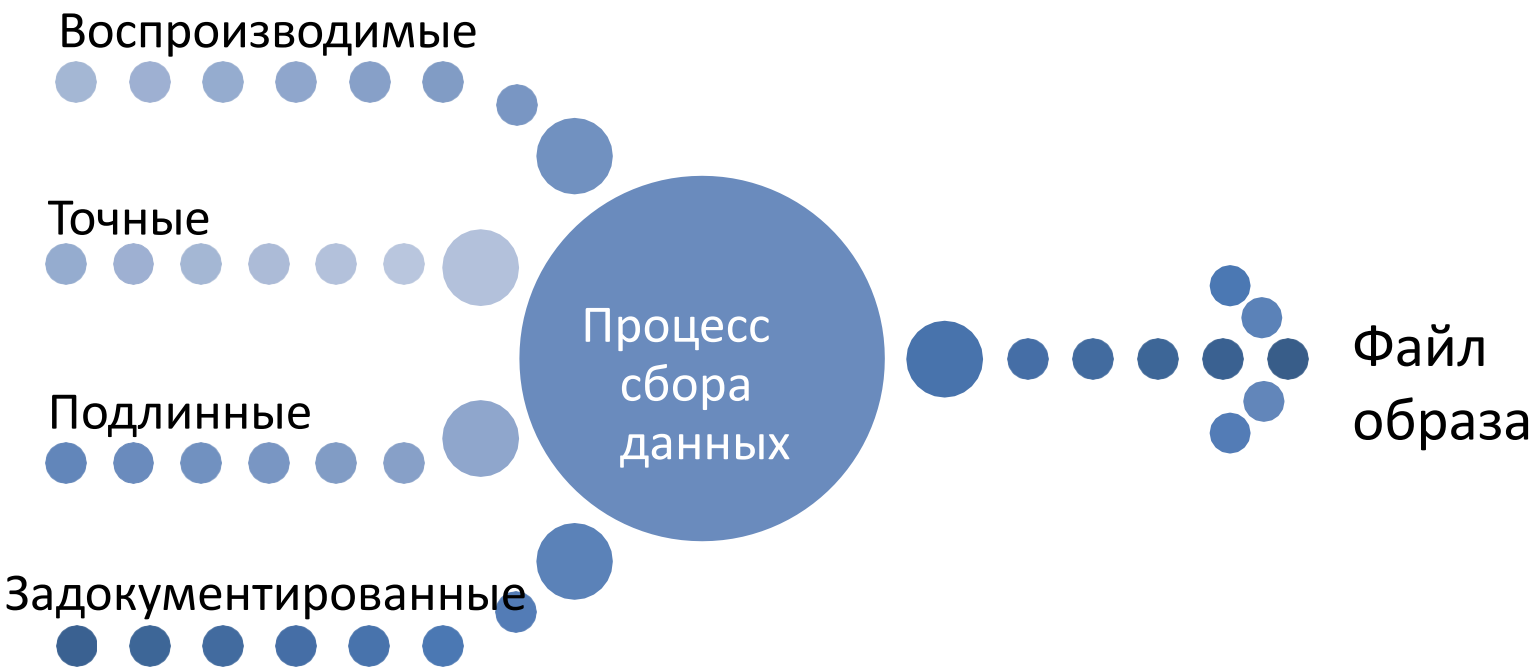
Аутентификация: Хэширование

- Области использования:
  - Верификация и аутентификация дубликата
  - Исключение файлов

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

Рекомендуемые аспекты для подтверждения целостности



Сохранение доказательств

Почему трудно собрать доказательства из социальных сетей?

- Мультимедиа
  - Могут содержать изображения, видео, текст, комментарии, лайки, координаты местоположений ...
- Бесконечная прокрутка
  - Можно прокручивать бесконечно
- Контент с привязкой внешних ссылок
  - 30% сообщений в социальных сетях содержат ссылки
- Сокращатели ссылок
  - Короткие ссылки (bit.ly, goog.le) могут со временем меняться или переставать работать

Почему трудно собрать доказательства из социальных сетей?

- Достоверность информации
  - Можно подделать
    - Например, Facebook-регистрация
  - Эксперт может получить информацию, но не может быть уверен, что информация верна
  - Можно получить информацию непосредственно из социальной сети
- Чувствительность информации
  - Может быть в любой момент удалена пользователем
- Копирование информации
  - Может быть легко скопирована на запоминающее устройство или сохранена как снимок экрана

Сохранение цифровых доказательств

- Ведите журнал регистрации всех действий
  - Сохранность вещественных доказательств при их передаче
- Аутентификация
  - Проверка целостности при помощи хэш-значений
- Рассмотрите возможность удаленного доступа
  - Лицо, получающее доступ к сети с разрешениями / без разрешений из внешних целевых объектов
- Рассмотрите возможность удаленного хранения в интернете
  - Может находиться в иностранной юрисдикции
  - Юридические вопросы?

Сохранение цифровых доказательств

- Моментальный снимок виртуальной памяти
  - Положительная сторона виртуализации и облачной среды
- Журналы
  - Если нарушение обнаружено слишком поздно, есть вероятность того, что журналы будут уничтожены в соответствии с политикой уничтожения

Сохранение цифровых доказательств

- Веб-страницы легко изменяются или удаляются
- Когда пользователь заходит на сайт (входит в систему, отправляет сообщение, совершает покупку ...), веб-сайт сохраняет его IP-адрес
  - При проведении разведки на основе открытых источников в Интернете выполняйте исследования с компьютера, который нельзя отнести к ведомству следователя
- Рекомендуется копировать веб-сайт:
  - Распечатка может быть единственной записью страницы
  - Записывайте соответствующие страницы, используя программное обеспечение для захвата видео
  - Скриншоты
  - Сохраняйте веб-страницу в браузере
  - Инструменты

Надежное хранилище данных

- Хранение данных пользователей на сервере поставщика ресурсов для облачных сервисов
  - Несанкционированный доступ к данным
    - Поставщик услуг
    - Хакеры
  - Изменение или удаление данных
    - Случайно или преднамеренно
  - Данные перемешиваются с данными др пользователей
    - Как сохранить конфиденциальность других участников при расследовании?
  - Законное владение данными

Сохранность доказательств при их передаче

- Одна из наиболее важных проблем в области цифровой криминалистической экспертизы
- Четко показывает, каким образом доказательства были:
  - Собраны
  - Проанализированы
  - Сохранены
- Начинается с получения физического контроля над доказательствами
  - в облачной криминалистике этот шаг невозможен
- Зависимость от поставщика ИТ-услуг при получении доказательств ставит под сомнение весь процесс расследования

Заключение цифровой криминалистической экспертизы

- Данные криминалистической экспертизы в расследованиях и судебных разбирательствах

Table of Contents

9 Alternate Data Streams (ADS)

Identify any alternate data streams and place the contents in an appendix including full path

10 Escripts

What scripts were run (details of the version of the script – could even hash it)

Where the evidence produced is to be found (i.e. on the accompanying CD or DVD (file locations) or Appendix

11 Text searches

Typically there will be a lit of search criteria. These should be listed here.

Then the results should be categorised according to the following criteria (only enter the search criteria at this point and the number of hits – from Encase or other forensic tool).

The results of the searches are in the appendix

11.1 No search hits

11.2 Search hits 1 – 200

11.3 Search hits 200 – 500

11.4 Search hits 500 – 1000

11.5 Search hits above 1000

12 Answers to specific questions asked by client

It may be that the client has asked a number of specific questions – they should be answered here and in the Appendix if appropriate

13 Files identified and found

These should be all put on the CD or DVD that accompanies the case.

Screenshots in the text are useful to demonstrate where the files were found or where the folders fit.

Современные данные криминалистической экспертизы

- Основные проблемы на сегодняшний день:
  1. Ограниченное время действия ордера на обыск
  2. Задержка в прохождении данных
- Почти в 80% случаев логическая выборка и предварительный просмотр используются для сортировки доказательств и подготовки файлов доказательств к более детальному анализу
- В разных странах разное время содержания подозреваемого под стражей

Заключение

- Цифровые доказательства отличаются от традиционных
  - Нелегко найти, непросто уничтожить
  - Активно развиваются инструменты, препятствующие криминалистическому расследованию
  - Сами цифровые доказательства также быстро развиваются
- Цифровая криминалистика отличается от традиционной
  - Традиционная криминалистика -> «сравнивающая» дисциплина
  - Цифровая криминалистика -> не с чем сравнивать
- Но при этом действуют одни и те же правовые нормы
  - Допустимость
  - Доказательная сила

Спасибо за внимание!

savina.gruicic@insig2.com