Россия, 2018

ЦИФРОВАЯ КРИМИНАЛИСТИКА

Повестка дня

- Введение в цифровую криминалистику
- Методология
- Стандартный порядок действий
- Вопросы управления
- Заключение

Введение в цифровую криминалистику


INSIG2
INTEGRIRANA SIGURNOST

Что это?

ИТ-безопасность и цифровая криминалистика

ИТ-безопасность

Цифровая криминалистика

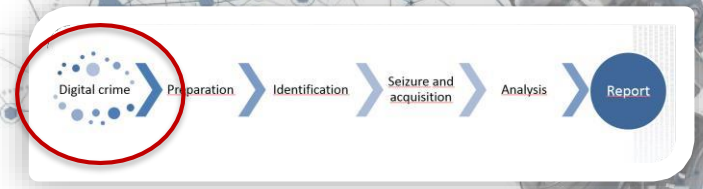
Отрасли


Мобильная связь
Облачная среда
ЦИФРОВАЯ КРИМИНАЛИСТИКА
Компьютер
Сеть

Цифровая криминалистика

Отрасль судебной науки, изучающая извлечение и исследование данных, обнаруженных на цифровых устройствах, зачастую в связи с компьютерными преступлениями.

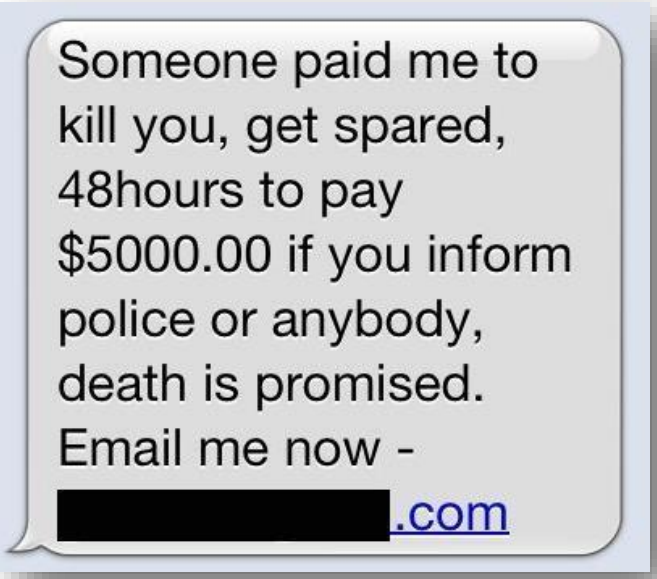
Цифровая криминалистика



Компьютерное преступление

Компьютерное преступление

- Любое незаконное действие с использованием электронного устройства
  - Инструмент
  - Цель



Виды дел в цифровой криминалистике

- Хакерская атака
- Кража
- Мошенничество
- Детская порнография
- Наркотики
- Шпионаж и государственная измена
- Организованная преступность
- Деньги на диске
  Замена диска
- Внутренние корпоративные расследования
- Исследования в области компьютерной безопасности
- Анализ причин неудачи или оценка ущерба

- Гражданские дела
- Нарушение договора
- Возвращение активов
- Нарушение конфиденциальности
- Нарушения законодательства и нормативных актов, регулирующих операции с ценными бумагами, и / или законов о компаниях
- Разногласия с персоналом
- Споры, связанные с авторским правом и другими правами на объекты интеллектуальной собственности
- Правовые обязательства по защите прав потребителей
  (и другие примеры ответственности без вины)
- Законодательство о защите данных
- …

- Законы о краже, включая мошенничество
- Нанесение уголовно-наказуемого ущерба
- Вымогательство
- Нарушение законодательства о компаниях, ценных бумагах, отраслевого и банковского законодательства
- Уголовные преступления, связанные с авторским правом и интеллектуальной собственностью
- Преступления, связанные с наркотиками
- Нарушения отраслевых стандартов
- Государственная и служебная тайна
- Нарушения закона о неправомерном использовании компьютера

INSIG2

Цифровые доказательства

Информация в цифровом виде, подтверждающая или опровергающая факт совершения преступления

Цифровые доказательства

- 2 проверки доказательств с целью обоснования их использования в судебных процедурах:

1. **Надежность**

   Являются ли доказательства надежными и не имеющими недостатков?

2. **Подлинность**

   Откуда получены доказательства?

4 ПРАВИЛА АСОП (Ассоциации старших офицеров полиции)

ASSOCIATION OF CHIEF POLICE OFFICERS

1. Целостность
2. Допустимость
3. Документация
4. Ответственность за весь процесс

Принцип 1

Действия со стороны правоохранительных органов или их ведомств не должны изменять данные на компьютере или носителях, которые впоследствии могут быть использованы в суде

- Проведение расследования исключительно (если это возможно) на копии
- Сохранение оригинала от разрушения
  - Представляемые в суд доказательства должны быть полными и неизмененными
- Обеспечение возможности повторного расследования
  - Проверка с помощью другого инструмента
  - Защита желает повторно провести процедуру
- Методы:
  - Контрольная сумма, хэширование, цифровая подпись, временные метки

Принцип 2

В ситуации, когда какое-либо лицо считает необходимым получить доступ к исходным данным, хранящимся на компьютере или на носителях, оно должно обладать достаточной квалификацией, а также быть способным доказать целесообразность и объяснить последствия своих действий

- Только в исключительных случаях расследование можно проводить на исходных данных
  - Такие расследования могут проводиться только компетентным лицом, которое при этом может доказать необходимость такого расследования
- Нельзя позволять некомпетентным сотрудникам проводить выемку
- Должны иметь соответствующие сертификаты, образование...

Принцип 3

Необходимо создать и сохранить журнал регистрации событий или иной учетный регистр всех процедур, применяемых к электронным доказательствам на компьютере. Независимая третья сторона должна иметь возможность изучить эти процедуры и получить такие же результаты

- Документируйте каждое свое действие
  - Например, устанавливая программу-клиент во время выемки мобильного телефона, объясните, почему это было необходимо
- Обеспечивайте сохранность доказательств при их передаче
- Доказательства должны быть воспроизводимыми

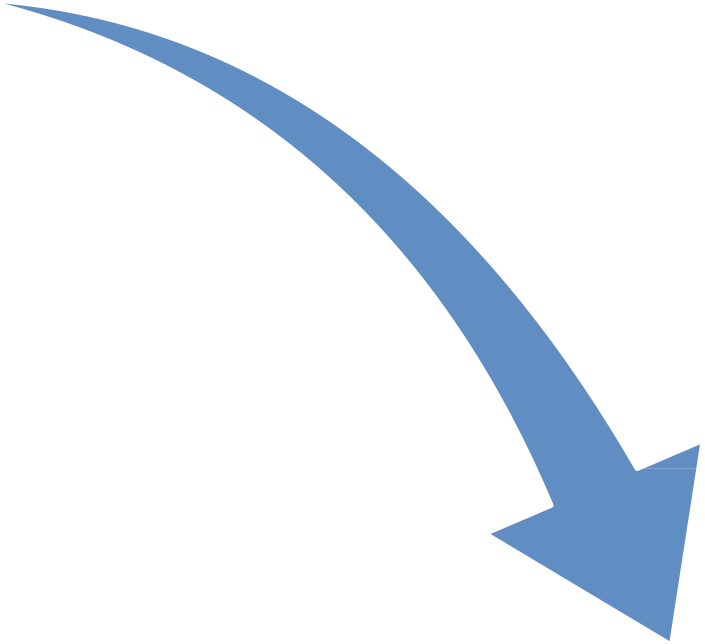
Принцип 4

Лицо, ответственное за расследование (следователь по делу), несет общую ответственность за обеспечение соблюдения законодательства и этих принципов

- Обеспечивает соблюдение всех 4 принципов

Когда начинается расследование?

Совершено преступление



Кто-то должен заметить...

СОП – Стандартная операционная процедура

- Ряд процедур, которые должны быть выполнены при проведении расследования
  - Шаги, которые необходимо предпринять во время сбора, обработки, получения, анализа, архивирования и предоставления отчетности
- У каждой компании, организации, учреждения имеются свои собственные процедуры
  - Например, https://www.cityofmadison.com/police/documents/sop/DigitalForensics.pdf

Законное использование Органы, ответственные за криминалистическую экспертизу

- **Службы быстрого реагирования**
  - Первые лица, прибывающие на место преступления
  - Несут ответственность за определение границ места преступления, его ограждение и сохранение изменяемых доказательств
- **Главный следователь**
  - Руководитель группы по расследованию происшествия
  - Обязанности:
    - Разрабатывает план реагирования на происшествие
    - держит в курсе руководство
    - обеспечивает поэтапное и эффективное проведение мероприятий по реагированию на происшествие
    - опрашивает и допрашивает свидетелей и подозреваемых

Законное использование
Органы, ответственные за криминалистическую экспертизу

- **Представитель службы информационной безопасности**
  - Предупреждает группу о возможных проблемах безопасности
  - Предоставляет информацию о конфигурации системы
  - Помогает оформить документы по месту происшествия
- **Технический специалист**
  - Создает резервные копии для проведения экспертизы
  - Предоставляет дополнительную информацию о конфигурации сети или целевой системы
- **Юридический представитель**
  - Обеспечивает, чтобы процедуры выполнялись в рамках закона
- **Отдел кадров**
  - Обеспечивает соблюдение политики организации
  - Тесно сотрудничает с юридическим отделом

4 основных аспекта выполнения операций в криминалистической лаборатории

4 основных аспекта выполнения операций в криминалистической лаборатории

- **Коммерческая деятельность**
  - Полицейская криминалистическая лаборатория должна демонстрировать ценность услуг и возврат вложений
  - Частнопрактикующий специалист должен оставаться конкурентоспособным
  - Корпоративная криминалистическая лаборатория должна демонстрировать эффективность и поддерживать высокие стандарты обслуживания клиентов и качества продукции
  - *УПРАВЛЕНИЕ КРИМИНАЛИСТИЧЕСКОЙ ЛАБОРАТОРИЕЙ - ЭТО УПРАВЛЕНИЕ ВЫГОДНЫМ ПРЕДПРИЯТИЕМ*

- **Технологический аспект**
  - Не отставать от развития технологий
    - Преступники часто имеют самые новые и самые сложные технологии

4 основных аспекта выполнения операций в криминалистической лаборатории

- **Научная практика**
  - Надежные, воспроизводимые, достоверные, объективные, последовательные и точные методики для объективного выявления фактов
- **Художественное творчество**
  - Интуиция и креативность
  - Интуитивное понимание взаимодействия людей и технологий

Подготовка

- Правило шести "П":

Предварительное Планирование и Подготовка Предотвращают Плохую Производительность

- Какова цель расследования?
- Какие цифровые доказательства вы рассчитываете найти?
- Дома или в офисе?
- Кто администратор?
- Есть ли сеть?
- Используется ли облачное хранилище?

Подготовка

- Выбор оборудования
  - КАМЕРЫ
  - Бумага, ручки, маркеры
  - Удлинительные кабели
  - Инструменты для криминалистического осмотра и обработки изображений (USB и CD)
  - Внешний жесткий диск
  - «*Лучше пусть оно будет и не понадобится, чем понадобится, а его не будет !!!*"

- Место преступления / ордер на обыск
  - Задействована сеть - Кто администратор?
  - Сохранение альтернативных доказательств (ДНК, отпечатки пальцев)
  - Безопасность прежде всего!

Подготовка

- Место преступления / ордер на обыск
  - Не думайте, что вы в безопасности, потому что это «компьютерное дело»,
  - Обеспечьте безопасность в зоне поиска
  - Не позволяйте никому находиться рядом с компьютером (компьютерами)
  - Не позволяйте никому прикасаться к клавиатуре.
- Опрос подозреваемого
  - Это ваш компьютер / у вас есть к нему доступ?
  - Какое имя учетной записи пользователя и пароль?
  - Кто еще пользуется компьютером?
  - У них отдельные учетные записи?
  - Шифрование / Учетные записи в интернете / Облачное хранилище

Соответствующее законодательство

- Существует большое количество соответствующих законов, правовых и нормативных актов, которые должны быть соблюдены при рассмотрении вопроса об изъятии и экспертизе электронных устройств
- Несоблюдение этих законов может привести к тому, что доказательства не будут приняты судом, а кроме того - к привлечению эксперта к судебной ответственности.

Облако – вопросы соблюдения требований

- Регулирование данных – со стороны третьих лиц
- Отсутствие стандартов в облаке
- Данные должны быть предоставлены юрисдикцией поставщика информационных услуг
- Юрисдикция
- Физический доступ невозможен

Итак, что это значит для вас?

- Будьте ответственными
  - Документируйте свои операции по обработке данных
  - Если вы храните личные данные, учитывайте законные основания такого хранения
  - Проверьте свои документы и формы согласия на соответствие требованиям
  - Любое лицо может потребовать от организаций удаления записей, содержащих его персональные данные

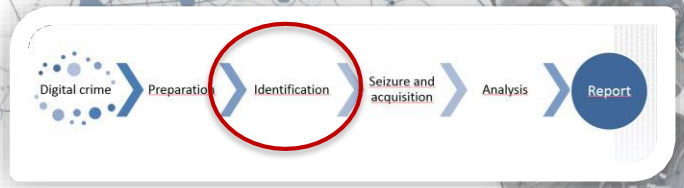
Зачем беспокоиться о законодательстве?

Шаг 1 - Преемственность

A = Полиция владеет на законных основаниях *** 1 = Обеспечивает законность изъятия представленного имущества, например, Закон о полиции и доказательствах по уголовным делам (PACE) (необходимо учитывать другие правовые аспекты, например, наличие согласия и косвенное вмешательство). При определенных обстоятельствах экспертиза может продолжаться, например, в случае «Непосредственного риска для жизни».**

Видеозапись суда присяжных

На месте преступления



Идентификация

А было ли вообще происшествие?

Какого вида происшествие?

Опрос подозреваемого

Изъять или анализировать на месте?

Выявить объекты и местоположения потенциальных доказательств

Зачастую то, что кажется атакой, может оказаться просто неисправностью системы или обрывом провода

Это ваш компьютер / у вас есть к нему доступ?

Какое имя учетной записи пользователя и пароль?

Кто еще пользуется компьютером?

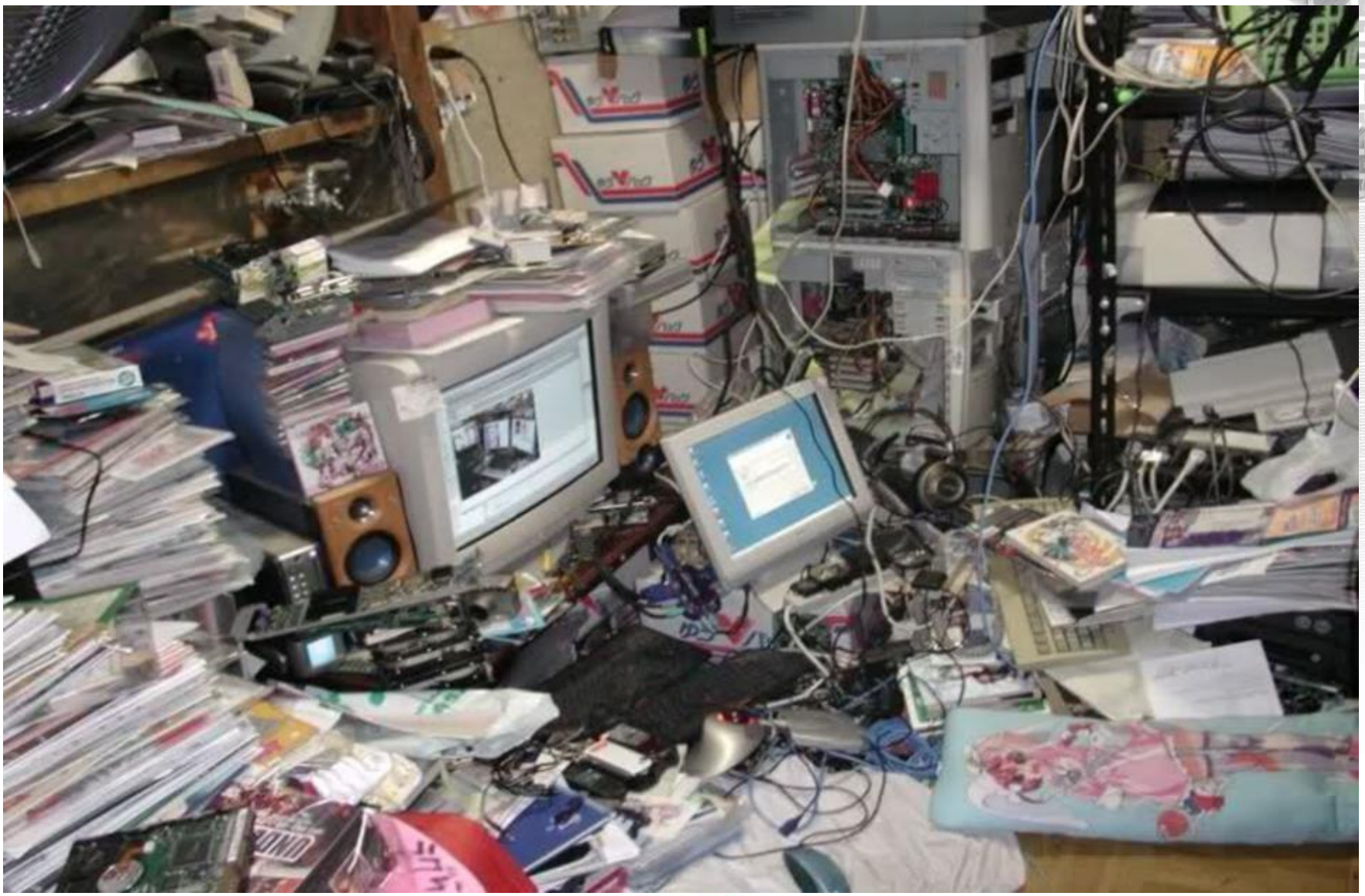
У них отдельные учетные записи?

Шифрование

Облачное хранилище

Жесткий диск, оперативная память, реестр, браузер, подключенные устройства, учетные записи электронной почты, серверы, облако ...

Идентификация




MY HOUSE
MY DISHWASHER
22
Minutes
MY REFRIGERATOR
-1° 38°
Freezer Refrigerator
DUET DRYER
1 25
Hour Minutes
DUET WASHER
Appliances
Energy
Settings


1:24
Where To?
View Map
Phone
Volume
Tools
GARMIN nüvi


Cloud Storage


SMART WATCH
2015/11/09
Mon


IN RS 7001


NOKIA

Сортировка - общий порядок действий

Правило № 1

- Если компьютер выключен, оставьте его выключенным

Правило № 2

- Если компьютер включен, *здесь возможны варианты ...*

Сортировка - общий порядок действий

- Документируйте
  - Что это?

    Марка, модель, серийный номер
  - В каком оно состоянии?

    Выключено / Включено / Отключено / Повреждено

    - Фотографируйте

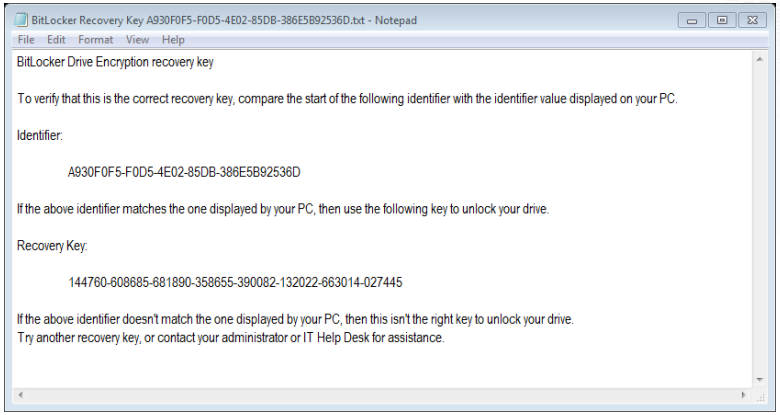
      Одна картинка стоит тысячи слов.

Сортировка - общий порядок действий

- Переместите мышь / нажмите клавишу «shift», чтобы вывести компьютер из «спящего» режима
- Документируйте и фотографируйте все окна.
- Проверьте панель задач на предмет открытых приложений.
- Проверьте наличие шифрования.
  - BitLocker
  - PGP - довольно хорошая конфиденциальность
  - TrueCrypt
  - Проверьте установленные программы!
  - Проверьте системный трей!
  - Проверьте иконки дисков!
  - Проверьте управление дисками!

Сортировка - общий порядок действий

- Если компьютер включен и разблокирован, сохраните дамп оперативной памяти!!
  - В ОЗУ можно найти много информации
  - Фотографии, последние файлы, сетевые соединения, процессы, вредоносные программы...
  - Подробнее рассмотрим этот вопрос позже ...
- По возможности сохраните ключи шифрования или создайте логический образ устройства в расшифрованной форме
- ДОКУМЕНТИРУЙТЕ!



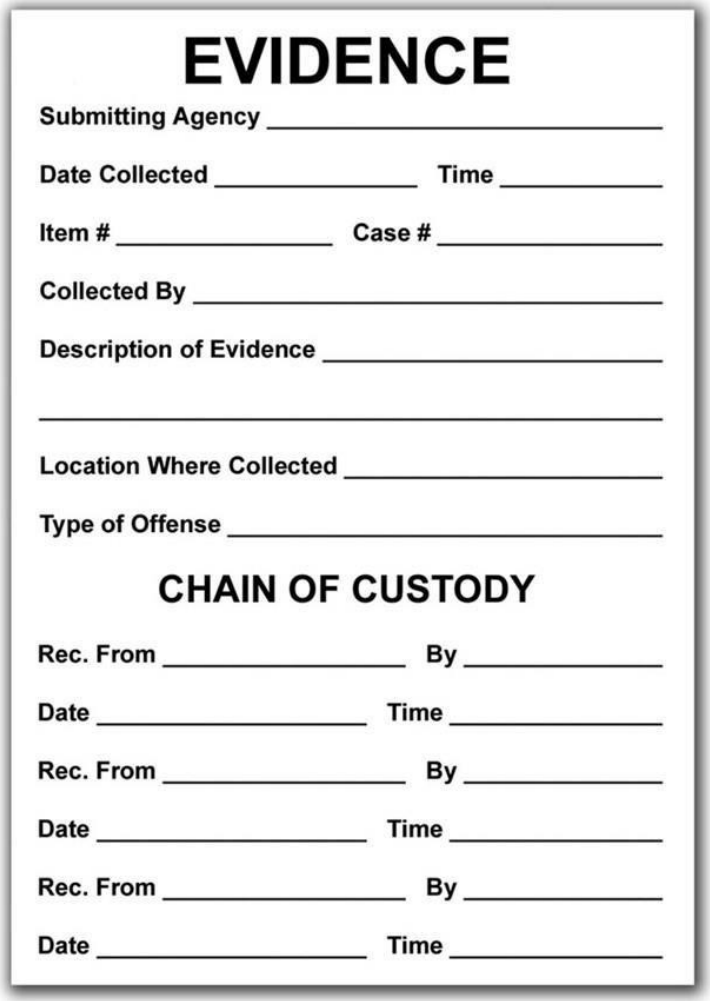
Варианты сортировки

- Создавайте образы дисков целиком или только их частей
  - Учитывайте особенности ордера
  - Объем экспорта данных
- Рабочие профили
  - Рабочие продукты браузера
  - Фотографии
  - Электронная почта
  - Информация о сети
  - …
- Live Box и Dead Box
- Пользовательские фильтры

Варианты сортировки

- Знайте, что вы ищете
  - Хэши
  - Расширения
  - Пути
- Планируйте заранее
  - Размер дисков и количество файлов
  - База данных NIST
  - Пароли и шифрование
- ДОКУМЕНТИРУЙТЕ!

Сохранность



EVIDENCE

Submitting Agency _____

Date Collected _____ Time _____

Item # _____ Case # _____

Collected By _____

Description of Evidence _____

_____

Location Where Collected _____

Type of Offense _____

CHAIN OF CUSTODY

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Изъятие

- Методы обработки на месте происшествия
  - Логический сбор данных
  - Физический сбор данных
  - Сортировка / Предварительный просмотр
- Изъятие и сортировка
  - Объем доказательств, которые нужно изучить
  - Технические ограничения
  - Вероятность наличия деструктивных процессов обработки данных, запущенных подозреваемым.

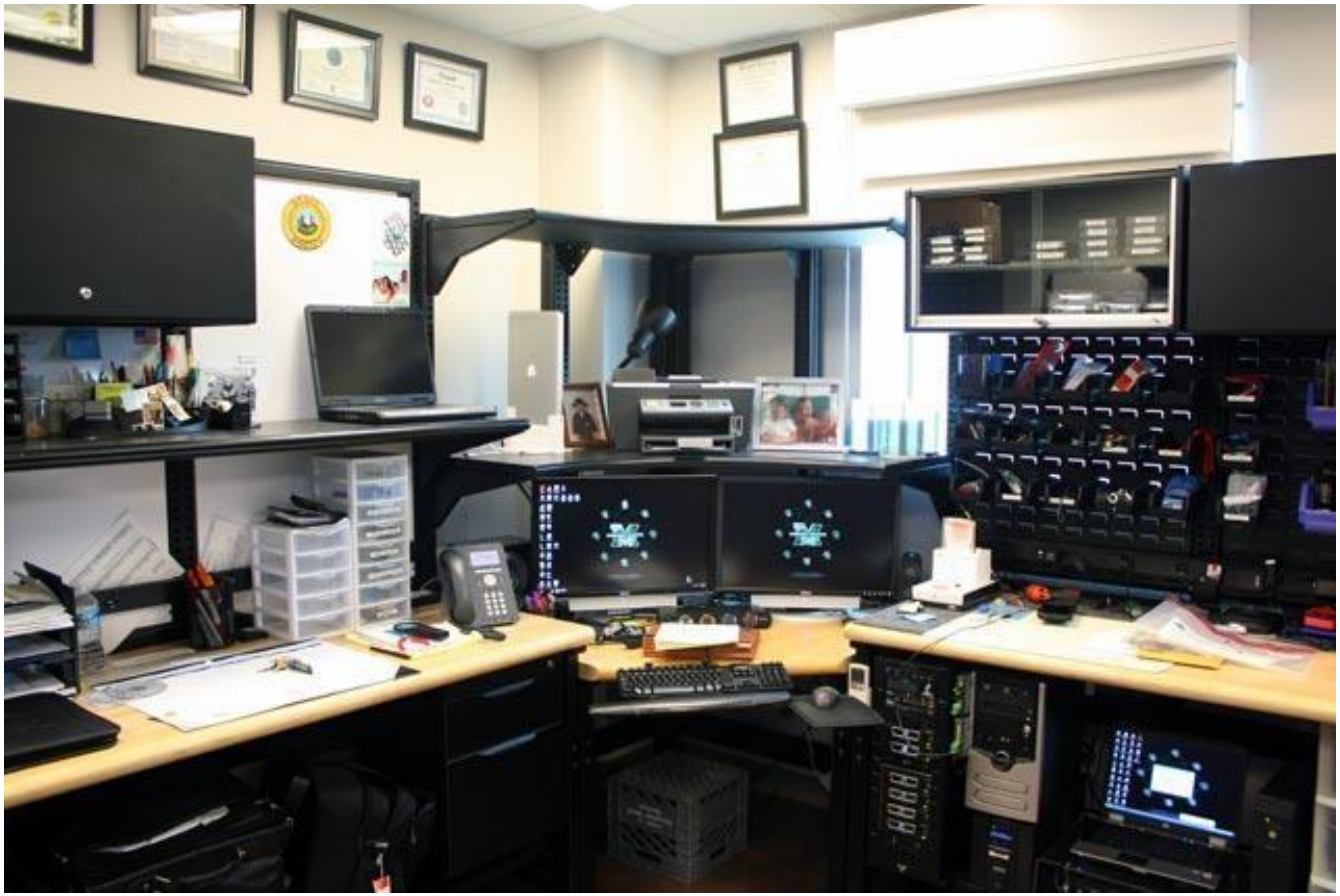
Изъятие


Защитить место преступления от несанкционированного доступа и повреждений
Упаковать
Запечатать
Проштамповать
Присвоить номер доказательства
Обеспечить сохранность доказательств при передаче

Упаковать и промаркировать

- Ставьте отметки на всех доказательствах, которые планируете изымать
  - Бумажные пакеты, этикетки, присваивание имен
  - Обеспечение сохранности доказательств при их передаче
- Надлежащие условия транспортировки
  - Чувствительные электронные устройства
  - Тряска в транспорте
- Лабораторная среда
  - Входной контроль
  - Температура внутри лаборатории

Лабораторный анализ



Аппаратное обеспечение в криминалистической экспертизе

- Блокировщики записей
- Мосты
- Рабочая станция Talino
- Комплексы Chinex
- JTAG-программаторы
- Считыватели карт памяти с защитой от записи

Программное обеспечение в криминалистической экспертизе

- Инструменты с открытым исходным кодом
- AccessData
  - Инструмент криминалистической экспертизы (FTK)
- Руководство/Opentext
  - EnCase
- Magnet
  - AXIOM, IEF
- Белкасофт
  - Belkasoft Evidence Center
- Cellebrite
  - UFED
- MSAB
  - XRY
- Многие другие

Проверка инструмента

- Сохранение целостности данных доказательств – в обязательном порядке
- Инструменты криминалистической экспертизы не должны каким-либо образом изменять данные.
- Перед использованием любого инструмента → проверка инструмента
- Эксперт должен лично убедиться, что:
  - Инструмент работает, как полагается
  - Инструмент дает правильные результаты
  - Инструмент не изменяет доказательства
- Кроме того, эксперт должен понимать внутреннее устройство инструмента, чтобы иметь возможность правильно интерпретировать результаты.
- Его компетенция и интерпретация доказательств могут быть поставлены под сомнение

Проверка инструмента

- Используйте в своем расследовании несколько инструментов
- Чтобы убедиться, что они работают правильно, вводите известные данные и проверяйте результаты
  - Проверка: результаты должны быть одинаковыми для всех инструментов

Сбор данных

- Извлечение данных доказательств с различных типов носителей
- Инструменты для сбора данных - программное обеспечение (криминалистические программы для обработки визуальной информации) / аппаратное обеспечение (блокировщики записи, криминалистические дубликаторы, другие криминалистические устройства)
- Криминалистическая среда

  загрузки
- Необходима проверка
- Целевые носители - жесткие диски для хранения криминалистических резервных копий

  - Стерилизация носителей

Сбор данных

- Программное обеспечение для сбора данных
  - EnCase, X-Ways, FTKImager, криминалистические дистрибутивы Linux (например, Paladin, SIFT)
  - Хэш до и после сбора данных → Проверка целостности доказательств
  - Создание криминалистических копий и файлов образов
- Монтирование образов
  - Образы могут монтироваться как физические устройства, и им присваивается номер диска в диспетчере устройств
  - Запуск действующей операционной системы с образа, созданного в ходе экспертизы

Стерильные носители

- Как известно, даже после удаления файлов остаются данные
- Если целевые диски для криминалистических резервных копий содержат остаточные данные, они могут быть ошибочно приняты за доказательства
- → Стерильные носители
- На стерильных носителях каждый байт перезаписывается с помощью известного или случайного шестнадцатеричного значения
- Стерильные с точки зрения криминалистики носители → Значение каждого байта равно 0x00
- Стерилизация = стирание

Стерильные носители

- Проверка стерильного носителя, перезаписанного со значениями 0x00, намного проще, чем работа со случайными числами или другими значениями
- Checksum64 - функция, которая обеспечивает метод проверки стерилизованного хранилища данных
  - Суммирует значения всех байтов на устройстве
  - Выдает 64-битный контрольный итог
  - Если носитель стерилизован надлежащим образом (со значениями 0x00), итоговая сумма должна быть 0000 0000 0000 0000
  - В противном случае результат будет иным, в зависимости от значений байтов
  - Результат не зависит от размера носителя, в отличие от хэш-функций, которые будут давать разные результаты для носителей разного размера

Стерильные носители

- Должны всегда использоваться при создании криминалистической копии данных на устройстве хранения, содержащем доказательства
  - "С диска на диск"
- Могут быть созданы с использованием различных инструментов
  - Инструменты криминалистической экспертизы (EnCase, X-Ways)
  - Криминалистические среды загрузки (дистрибутивы Linux - Paladin, Raptor)
  - Используемые в криминалистике устройства зачастую имеют функцию стирания жесткого диска
  - Реализуйте функцию стирания диска самостоятельно, на языке программирования по своему выбору
    - Не забудьте проверить инструмент и носитель

Криминалистические резервные копии и образы

- Эксперты-криминалисты никогда не должны работать на рабочей системе или исходном носителе
- Необходимо, по возможности, делать криминалистическую резервную копию исходных материалов
- Криминалистическая резервная копия содержит все данные с устройства хранения
  - Файлы и папки
  - Основную загрузочную запись, структуру разделов
  - Удаленные файлы
  - Неиспользуемое пространство
  - Нераспределенное пространство

Криминалистические резервные копии и образы

- Два основных вида криминалистических резервных копий
  - Криминалистическая копия - содержимое доказательств копируется на стерильный диск такой же или большей емкости, а оставшаяся часть дискового пространства заполняется значениями 0x00
    - "С диска на диск"
  - Криминалистические файлы образов/доказательств - содержимое доказательств копируется (копирование в виде битового потока) в файл на целевом диске
    - "С диска в файл"
    - Различные виды файлов доказательств (образов) (EnCase E01/Ex01, Linux dd, AFF, и т.д.)

Хэширование и массив хэшей

- Хэширование = представление цифрового контента в виде уникального числового значения, сгенерированного с использованием односторонней хэш-функции
- Хэш-значение = цифровой отпечаток части данных (файл, образ, блок данных, физическое устройство и т. д.)
- Малейшее изменение (1 бита) входящих данных приводит к большим изменением исходящих данных

Хэширование — области применения

- Проверка хэша
  - Совпадение хэш-значений может доказать, что данные доказательств не были изменены в ходе экспертизы
  - Хэш до сбора данных - состояние носителей до начала сбора информации
  - Хэш после сбора данных - состояние носителей после завершения сбора информации
  - Если все значения совпадают → данные доказательств не были изменены
- Проверка подлинности криминалистической резервной копии
  - Сравнение криминалистической резервной копии (файла образа) с исходными данными
  - Совпадение хэш-значений означает, что данные образа соответствуют исходным данным

Хэширование — области применения

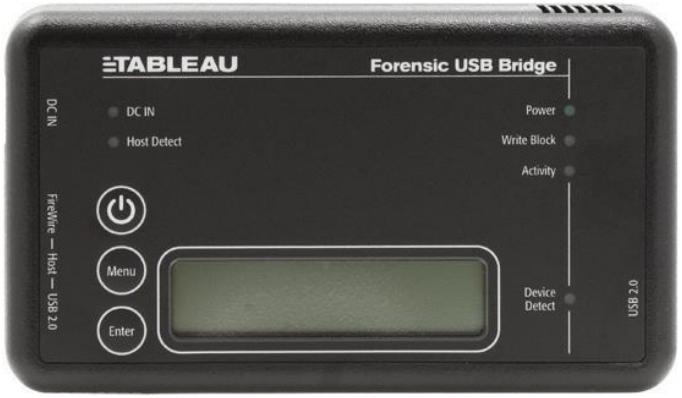
- Сравнение файлов с помощью их хэш-значений
- Сопоставление файлов
  - Сравнение хэшей файлов для подтверждения наличия несанкционированных файлов
  - Маркировка файлов с соответствующими хэш-значениями для дальнейшего изучения
- Исключение файлов
  - Сравнение хэш-значений файлов с известными файлами (например, системными или программными файлами)
  - Исключение таких файлов из экспертизы → Уменьшение объема данных, подлежащих изучению
- Нечеткое хэширование - хэширование дискретных блоков файловых данных вместо всего файла → Обнаружение несанкционированных файлов, даже если были произведены небольшие изменения

Блокировка записи

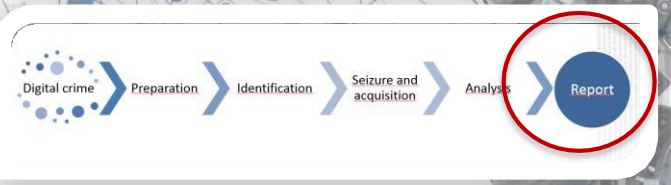
- Эксперты должны убедиться, что доказательства не были изменены во время проведения экспертизы
- Необходимо сохранить исходные доказательства
- Команды, которые производят операции с содержимым памяти устройства, не должны иметь доступ к устройству
- Режимы защиты:
  - Аппаратная защита
    - Переключатели в режим «только для чтения», вкладки «Блокировка», устройства хранения данных с защитой от записи
  - Программная защита
    - Дистрибутивы Linux, которые монтируют устройства как доступные только для чтения
    - Перехват вызовов API-функций Windows, которые выполняют запись на диск
    - Внесение изменений в ОС Windows
    - Внесение изменений в BIOS - интерфейсы, доступные только для чтения

Блокировка записи

- Защита прошивки
  - Независимо от ОС
  - Физическое устройство со встроенной прошивкой, которая предотвращает доступ команд записи к контроллеру устройства
  - Физическое устройство, которое создает криминалистическую копию или образ на целевом устройстве
  - Производители: Tableau, WiebeTech, LogiCube, и др.



Блокировка записи


Digital crime
Preparation
Identification
Seizure and acquisition
Analysis
Report

Отчет

Отчет

Достоверность и точность

- Краткие выводы расследования
  - Основная форма для документирования каждого действия
- Форма выемки электронного устройства
  - Информация с устройства
- Сохранность доказательств при их передаче
  - С момента выемки до момента представления в суде
- Контрольный список электронных устройств
  - поэтапный процесс выемки

Отчет

- Документируйте каждый этап цифровой криминалистической экспертизы, результаты анализа и выводы
- Четко и лаконично
- Цель: позволить читателю использовать информацию, не понимая, как была представлена информация или что она означает → *читатели-непрофессионалы*
- Будьте уверены в том, что вы используете надежные, воспроизводимые и точные методы, основанные на передовых практиках и процедурах!

Элементы отчета

1. Идентификация

- Электронных устройств

2. Сбор

- Цифровых доказательств

3. Анализ

- Доказательств

4. Представление

- Полученных результатов

Что это теперь?

САМЫЕ НАДЕЖНЫЕ СВИДЕТЕЛИ

INSIGT

СЛУЧАЙ ИЗ ПРАКТИКИ - ДЖУЛИ АМЕРО

Что пошло не так?

Когда не соблюдаются принципы и стандарты цифровой криминалистики

...

Штат Коннектикут против Джули Амеро

- Вызывающий тревогу недостаток в понимании юридическим и судебным сообществом цифровых доказательств
- Правовая неграмотность в вопросах цифровых доказательств может оказать серьезное влияние на жизнь человека
  - Показывает, как общее отсутствие понимания цифровых доказательств может привести к тому, что невиновный обвиняемый будет несправедливо осужден
- Чтобы понять, почему, с точки профессиональной компетенции, необходимо ознакамливаться с цифровыми доказательствами

История согласно данным, полученным от Школьного округа и Прокурора

- 19 октября 2004 г., учитель на замену Джули Амеро провела целый день в Интернете, рассматривая порнографические сайты
- В течение дня учащиеся оставались без внимания
  - Нанесение вреда моральному состоянию детей

История со слов Джули Амеро

- 19 октября 2004 г. Джули Амеро заменяла учителя
- Учитель запустил для нее компьютер и выполнил вход в систему
- Ненадолго вышла из класса, а когда вернулась, 2 ученика использовали учительский компьютер
- Амеро заметила порнографические изображения, появляющиеся на экране
- Ей сказали не выключать компьютер
  - Не знала, как это сделать
- Развернула экран и попыталась закрыть изображения.
  - Всякий раз, когда она закрывала одно окно, открывалось новое

История со слов Джули Амеро

- Во время первого урока в классе присутствовала ассистент по языку жестов
  - Попросила ее присмотреть за классом, пока она сходит за помощью
  - Ассистент отказалась
- Во время обеда она побежала в учительскую и попросила о помощи
  - Дверь не закрыла, поскольку у нее не было ключей
  - Ей сказали, что окна всплывают все время, и не стоит беспокоиться
- Вернулась в класс, а помощь не прибыла
- Сообщила о проблеме директору и заместителю директора

Риск нанесения детям травмы
Сборник законов штата Коннектикут, Раздел 53-21 (a) (1)

*«Любое лицо, которое умышленно **или** противоправно создает или допускает возникновение такой ситуации для ребенка в возрасте до шестнадцати лет, в которой может быть нанесен вред моральному состоянию такого ребенка, должно понести наказание»*

Обвинения, зачитанные Джули Амеро
Сборник законов штата Коннектикут, Раздел 53-21 (a) (1)

*«Ответчик умышленно **и** противоправно создал для ребенка в возрасте до шестнадцати лет такую ситуацию, в которой может быть нанесен вред моральному состоянию указанного ребенка»*

«ИЛИ» в сравнении с «И»

- Умышленно **ИЛИ** противоправно
  - Умышленно: нужно доказать психологический элемент намерения
  - Противоправно: не требует конкретного намерения
- Умышленно **И** противоправно
  - Обвинение обязано доказать намерение
  - Судья должен был сделать поправку
  - Чтобы доказать наличие умысла, присяжные должны были определить, как себя вел человек, и в каких обстоятельствах проявлялось это поведение

Штат Коннектикут против Джули Амеро

- Джули Амеро вынесен обвинительный приговор по 4 пунктам обвинения в подвергании риску нанесения травмы ребенку
  - Предусматривает до 40 лет тюремного заключения
    - Каждое обвинение - до 10 лет лишения свободы
- После долгих лет страданий из-за пребывания под подозрением, Джули признала себя виновной в нарушении общественного порядка
  - Отозвана лицензия на преподавание
  - Заплачен штраф
  - Множество проблем со здоровьем
    - Включая трагический выкидыш

Что пошло не так?

Джули Амеро, ответчик

- Не получила соответствующих инструкций по использованию компьютера: в частности, ей сказали **не выключать** компьютер
  - Она не выключила и даже не знала, как это сделать
  - Повернула компьютер к стене
  - Удерживала учащихся на расстоянии
- Пошла за помощью
  - Не могла закрыть дверь, поскольку у нее **не было ключей**
  - В тот же день сообщила заместителю директора, а на следующий день - директору.

Скотт Файн, директор

- **Скрыл информацию**
  - Не сообщил следователю о докладе Амеро его заместителю и ему.
  - Эта информация продемонстрировала бы, что ее доступ не был преднамеренным
- Опросил 60 учащихся, которые были в классе в тот день
  - 10 видели некоторые непристойные материалы, 8 увидели мягкую эротику

Учащиеся

- 11 были опрошены следователем
  - 1 ничего не видел, 8 видели мягкую эротику, 2 видели материалы, вызывающие большее беспокойство
    - Оба заявили, что фотографии были «***маленькими***», а они сидели на таком месте, что Амеро не заметила, что они все видят
  - 6 учащихся дали показания
    - 2 сообщили, что видели на экране «***кучу маленьких картинок***»
    - Посмотрели на экран **после** того, как другой учащийся сказал им, что учитель смотрел порнографию
- Сообщили, что Амеро приложила определенные усилия, чтобы ограничить их обзор
- Амеро были предъявлены обвинения только по 4 пунктам

Дэвид Смит, адвокат обвинения

- Низкий уровень компьютерной грамотности
- Не смог обеспечить сохранность доказательств при их передаче
- Не было надлежащего понимания того, **как представлять** цифровые данные в соответствии с фактическими событиями
  - Неизвестно, соответствуют ли изображения, показанные присяжным, тем, которые видели дети
    - Возможно, что изображения не отображались на мониторе, поскольку для этого необходимо было прокрутить вниз страницу
  - Отображались полноэкранные порнографические изображения
    - Не соответствует уменьшенным изображениям всплывающих окон

Дэвид Смит, адвокат обвинения

- Не смог представить четкую последовательность событий
  - Время, когда дети фактически были в классе
  - Время, когда они видели изображения
- Не смог определить, какого размера были увиденные изображения.
- Не смог определить, какие изображения видели дети

Джон Ф. Кочео, адвокат защиты

- Низкий уровень компьютерной грамотности
  - Вопросы, содержащие такие выражения, как «паразиты»,
- Не выдвигал аргументов против процедуры расследования
- Не оспаривал сохранность доказательств при их передаче
- Не ставил под сомнение достоверность на основании различий во временных метках
- Не ставил под сомнение достоверность экспертных заключений, описывающих поведение вредоносных программ
- Не возражал, когда обвинение показывало полноразмерные порнографические изображения
- Не предоставил копию экспертного заключения прокурору

Херб Хорнер, свидетель-эксперт со стороны защиты

- Получил жесткий диск и сделал копии для своего расследования
- Его показания отклонены судьей, поскольку они не были заранее представлены обвинению
- Информация, представленная Хорнером, являлась доказательством наличия шпионской программы на компьютере, которая генерировала всплывающие окна с порнографическим содержимым

Роберт Харц, IT-менеджер

- Предоставил информацию о журналах брандмауэра с историей посещенных сайтов
  - Не проверил промежутки времени между загрузками страниц
  - Не проанализировал схему доступа, чтобы определить, было ли появление случайным или запланированным
- Отчет по первоначальному анализу журналов, проведенному 21 октября 2004 г.
  - С 8:38 до 14:46 доступ к Интернету осуществлялся постоянно
  - Несколько перерывов в использовании Интернета (время перемен и обеда)
  - Посещались различные сайты - от электронной почты до сайтов путешествий и причесок
- Встретился со следователем 27 октября 2004 г.
  - Не сказал, что истек срок действия лицензии

Роберт Харц, IT-менеджер

- Не проверил компьютер на наличие вредоносных программ
- Не выполнял регулярное обновление баз антивируса
  - Устарели минимум на 3 месяца
- Не установлена антишпионская программа в брандмауэре клиента
- Истек срок действия школьного фильтра контента
  - Не сообщил об этом следователю
- Разница временных меток между сервером электронной почты и компьютером составляла
  - 10 или 12 минут до или после
  - Может иметь решающее значение для свидетельских показаний:
    - До - указывает на то, что учащиеся смотрели изображения, пока Амеро отсутствовала в классе
    - После - указывает на то, что это происходило в присутствии Амеро

Марк Лоунсбери, офицер полиции

- Лично скопировал и проверил жесткий диск
  - Исследовал исходный жесткий диск на действующей системе вместо копии
  - Не соблюдены отраслевые стандарты в части дублирования жесткого диска
  - Жесткий диск скопирован при помощи *Ghost*
- Представил доказательства того, что компьютер использовался в последний раз 26 октября 2004 г.
- Не опросил сотрудников
- Не проверил компьютер на наличие вредоносных программ

Марк Лоунсбери, офицер полиции

- Свидетельствовал в суде, что Амеро должна была специально заходить на сайты, чтобы это зафиксировалось в журналах
  - **ОШИБОЧНО**!
    - Все сайты попадают в журнал, независимо от того, осуществлялся к ним доступ намеренно или из-за вредоносных программ или «программ-порноловушек»
    - Веб-разработчики могут настроить автоматическое открытие веб-страниц при посещении определенных сайтов (например, рекламные всплывающие окна и рекламные ролики)

Марк Лоунсбери, офицер полиции

- Заявил в суде, что красный цвет временных файлов Интернета обязательно указывает на то, что веб-сайт посещался и открывался преднамеренно
  - **ОШИБОЧНО!**
    - Веб-разработчики могут изменять цвет ссылок
    - Сами пользователи или операционные системы также могут изменять цвет ссылок
- В HTML-коде веб-страницы Female Sex Enhancers содержалась команда изменить цвет шрифта на красный
  - Красный цвет был задан, а не изменился в результате посещения

Судья

- Отказал в даче полных показаний свидетелем-экспертом со стороны защиты
  - Из-за того, что информация не была представлена заранее
- Не подвергал сомнению методы представления изображений
- Вынес решение, что экспертное заключение Харца, имеющего 20-летний опыт работы, является достаточным

Краткие выводы

Неудовлетворительное расследование

- Районный директор по вопросам информационных технологий
- Следователь по компьютерным преступлениям

Непредставление информации

- должностными лицами школы следователю в отношении сообщений и действий Амеро

Недостоверные показания

- Следователь по компьютерным преступлениям
- IT-менеджер

Показ непристойных изображений

- Нет оснований считать, что это были сайты, которые на самом деле видели учащиеся

Не было предоставлено экспертное заключение

- Адвокатом защиты прокурору
- Привело к исключению доказательств

Рекомендации

- Передовая практика включает проверку на предмет корреляции событий, которая ищет причины рассматриваемых действий
  - Ненадлежащие процедуры экспертизы привели к упущению фактов
  - Не выполнялся поиск вредоносных программ
- Полный анализ ситуации
  - Что человек делал перед инцидентом
  - Как он отреагировал
  - Определить наличие вредоносных программ
  - Просмотреть журналы, чтобы определить, была ли схема доступа случайной или обычной