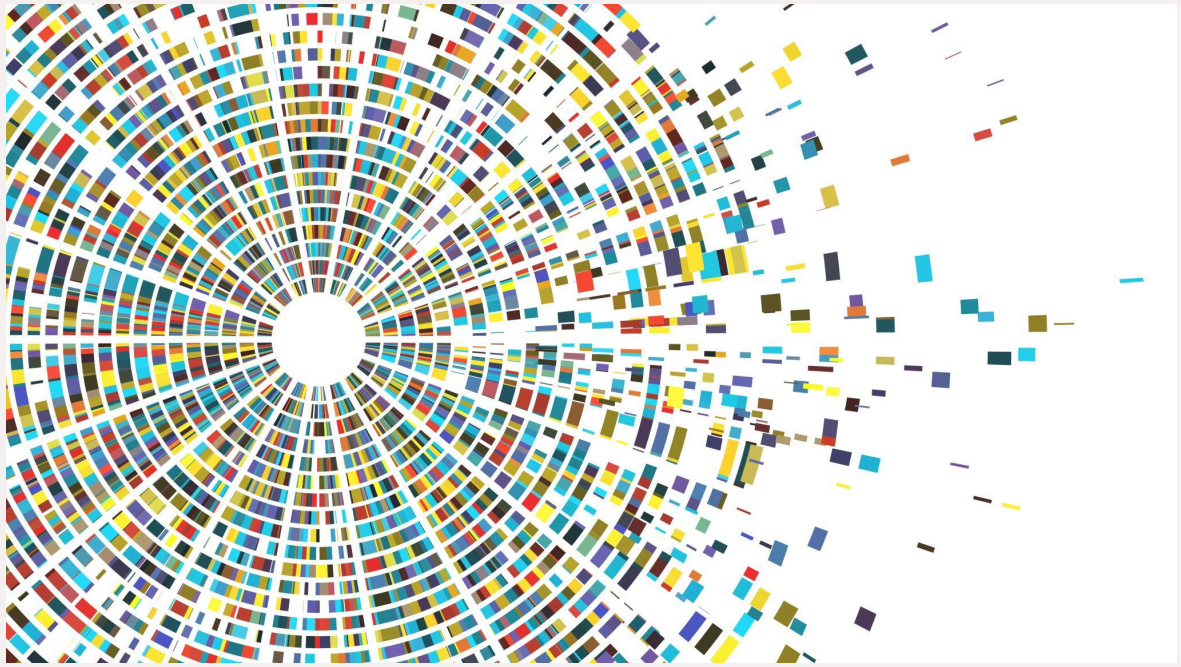
Digital Forensics (**на практике**)

ОБЗОР ИНСТРУМЕНТОВ ДЛЯ СБОРА ИНФОРМАЦИИ



- Цифровая криминалистика - это область криминалистики, которая занимается исследованием и расследованием преступлений, связанных с использованием компьютеров и цифровых устройств. Она включает в себя сбор, анализ и интерпретацию электронных данных и информации с целью раскрытия и предотвращения киберпреступлений, включая хакерские атаки, мошенничество, цифровой след и другие виды преступлений, связанные с технологиями и интернетом.

- Цифровые криминалисты используют специальные инструменты и методы для изучения электронных следов, включая анализ жестких дисков, мобильных устройств, сетевых данных, электронной почты и других цифровых следов. Они также могут свидетельствовать в суде и помогать в расследовании различных видов преступлений, в которых используются компьютеры и интернет.

- Цифровая криминалистика становится все более важной в наше время, поскольку киберпреступность и киберугрозы становятся все более распространенными и сложными. Эта область также включает в себя соблюдение законов, связанных с использованием и защитой данных в цифровом мире.

Цели цифровой криминалистики

Зависит от масштаба и специфики расследуемого случая

- Методы анализа и обеспечения текущего состояния цифрового артефакта
- Поддержка или опровержение предложений о том, как было совершено преступление
- Определение объема утерянных данных
- Расследование вторжений в компанию/организацию
- Принятие мер по улучшению защиты компьютерных систем

Цифровая криминалистика

«Компьютерная криминалистика –это эквивалент обследования места преступления или вскрытия тела жертвы». James Borek, 2001

«Компьютерная криминалистика –это процесс идентификации, сохранения, анализа и представления цифровых улик юридически приемлемым образом».Rodney McKemmish, 1999

- Разновидности:
- Сетевая криминалистика
- Мобильная криминалистика
- Криминалистика баз данных
- И т.д., и т.п.
- Криминалистика АСУ ТП

Где могут быть цифровые улики ?

Цифровые улики можно определить как «любые данные, которые хранятся или передаются, могут быть значимыми для расследуемого дела».

Примеры того, где могут находиться цифровые улики:

- Жесткие диски
- Оперативная память
- Сетевые пакеты
- Журналы событий логических контроллеров
- Сообщения электронной почты
- Документы
- И т.д.

Принципы цифровой криминалистики

Как провести успешное цифровое расследование?

- Свести к минимуму потерю данных при сборе цифровых улик.
- Делать записи обо всем.
- Анализировать все собранные данные.
- Работать с персоналом.
- Максимально подробно проверить полученные результаты.

Этапы цифрового расследования

Цифровое расследование, также известное как цифровая криминалистика, включает в себя несколько этапов, которые следует выполнять для успешного анализа и расследования цифровых угроз и преступлений. Вот основные этапы цифрового расследования:

- **Подготовка**:

  Определение целей расследования и формулирование задач.

  Составление плана расследования, включая выделение ресурсов и определение методологии.

  Получение необходимых правовых документов и разрешений, если это требуется.

- **Сбор данных**:

  Идентификация и сбор цифровых следов, включая данные с компьютеров, мобильных устройств, сетей, серверов и других источников.

  Создание копий данных для анализа, чтобы сохранить целостность оригинальных данных.

  Документирование и упаковка физических устройств, если они являются частью доказательств.

- **Анализ данных**:

  Расшифровка и интерпретация собранных данных.

  Идентификация цифровых следов, включая файлы, сообщения, журналы событий и другую информацию.

  Выделение ключевых фактов и доказательств.

  Анализ метаданных, таких как даты, время и местоположение.

- **Исследование и реконструкция**:

  Построение логических связей между найденными доказательствами.

  Реконструкция событий и действий, связанных с преступлением.

  Идентификация потенциальных подозреваемых и свидетелей.

- **Документирование**:

  Создание подробных отчетов о расследовании, включая описание методологии, найденных доказательств и выводов.

  Ведение журнала всех действий и принятых мер, чтобы обеспечить прозрачность и законность процесса.

- **Подготовка к суду**:

  Подготовка к представлению доказательств в суде, включая подготовку экспертных заключений и свидетельских показаний.

  Обеспечение юридической допустимости собранных и анализируемых данных.

- **Завершение расследования**:

  Подготовка и передача дела в компетентные органы (полицию, прокуратуру, суд, КНБ) для дальнейшего рассмотрения и принятия решений.

- **Мониторинг и обучение**:

  Мониторинг результатов расследования и оценка эффективности принятых мер.

  Обучение и улучшение навыков и методов на основе опыта и новых технологических изменений.

- Эти этапы представляют общий обзор процесса цифрового расследования, но они могут быть адаптированы в зависимости от конкретной ситуации и характера преступления. Они также могут варьироваться в зависимости от требований закона и специфики организации, выполняющей расследование.

Реагирование на инциденты

Реагирование на инциденты (Incident Response) - это процесс, в рамках которого организация разрабатывает и реализует план действий для выявления, анализа и реагирования на инциденты информационной безопасности, с целью минимизировать их воздействие и восстановить нормальную работоспособность систем и данных.

Процедура реагирования на инциденты

Успешность цифровой криминалистики во многом зависит от шагов по борьбе с инцидентом

- Необходимо наличие заранее определенных планов и стратегии со стороны как технических, так и юридических подразделений
- Теперь все зависит от того, когда инцидент произойдет
- Отсутствие обнаружения не означает отсутствия атак
- Вид бизнеса не играет роли. Например, Stuxnetи последняя атака RuAttack
- Разработано много стандартов и нормативов по работе с инцидентами:
  - ISO 27035:2011 “Information security incident management”
  - NIST, “Computer security incident-handling guide”

Этапы реагирования на инцидент

Этапы реагирования на инцидент... подготовка

- Обучение сотрудников
- Внедрение методов мониторинга
- Подготовка лабораторий, ПО, аппаратного оборудования, ресурсов, планов и политик
- Система отслеживания инцидентов
- Список контактов внутри и вне организации, правоохранительные органы
- Рабочий график 24/7
- Тренировки по безопасности, учения
- Различные каналы коммуникаций
- Документация по нормальному поведению систем и сетей в среде
- Программа осведомленности о безопасности для всех пользователей

Этапы реагирования на инцидент... подготовка

Создание резервных копий содержимого носителей информации устройств, включая программы PLC (Важно!) и прошивку (при возможности).

Инструменты

- Ноутбук криминалиста
- Устройства хранения данных
- Устройства копирования
- Блокираторы записи
- Кабели, переходники, адаптеры
- Блокнот
- Что ещё?

Сумка с набором инструментов

Методы защиты для предотвращения инцидентов

Этапы реагирования на инцидент... Идентификация

Это инцидент или только событие?

Требуется первичный технический анализ для идентификации аномалий в среде

Определение типа, масштаба и величины инцидента.

Сложности:

- •Различные каналы оповещения – как внутренние, так и внешние
- •Необходим анализ большого числа поступающих оповещений, среди которых может оказаться много ложных срабатываний
- •Для анализа нужны опытные специалисты

Сохранять спокойствие.

Сообщить руководству, руководителю ИБ, при необходимости в правоохранительные органы

Сообщить партнерам / клиентам, которых затрагивает инцидент

Этапы реагирования на инцидент... Идентификация

Назначить главного ответственного.

Обеспечить политику доступа только к необходимой информации.

В случае компрометации сети или машины:

- удостовериться, что угроза не имеет функционала распространения
- переключить на резервные устройства
- переключить на альтернативный/дополнительный канал связи
- внедрить сетевой мониторинг
- организовать сбор улик в реальном времени

Попросить все группы вести записи о своих действиях.

Сразу после подтверждения инцидента изменения файлов или ресурсов не допускаются.

Обеспечить сохранность улик.

Этапы реагирования на инцидент... Локализация

Должна быть выполнена до того, как атака распространится на ресурсы или приведет к более масштабному воздействию

Все сводится к принятию решений. Что нужно сделать, чтобы локализовать инцидент?

Подготовьте стратегии с утвержденными действиями, сообразными масштабу угрозы

Для каждого инцидента нужна своя стратегия локализации

Локализация инцидента с распространением вредоносного ПО отличается от локализации, например, атаки инсайдера

Неверная локализация может привести к потере доказательных данных

Этапы реагирования на инцидент… Локализация

Качественный сбор улик обеспечивает качество анализа

Улики, допустимые в качестве доказательства в суде – отдельный класс

Запись всей документальной информации – серийные номера, модели, IP-адреса и все другие метаданные

Цепь обеспечения сохранности улик – запись всех данных по передаче улик.

Запись причины передачи, имя получателя, временные метки и место

Различные системы имеют различную структуру

Этапы реагирования на инцидент... Устранение

Удалить все вредоносные компоненты инцидента

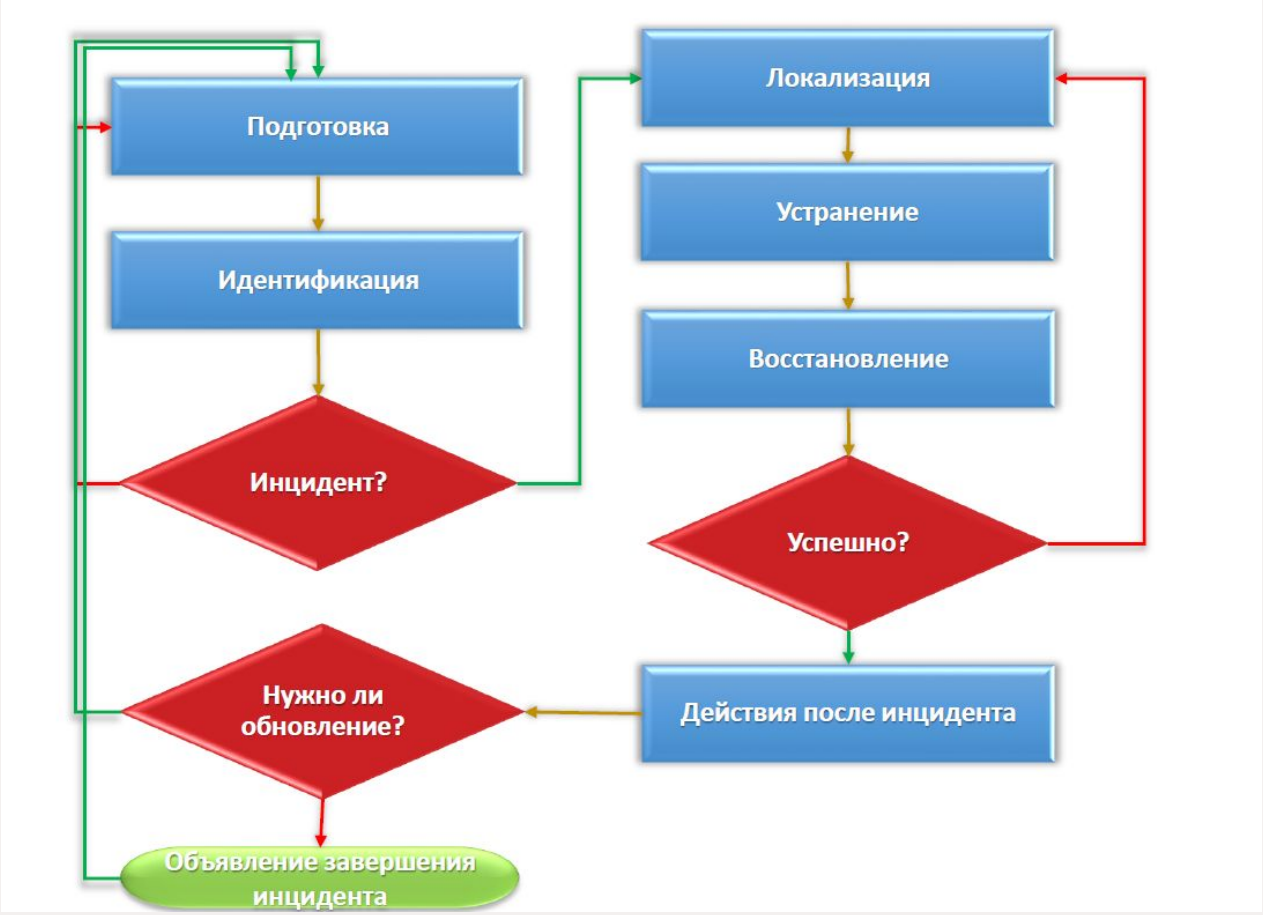
Принять меры для предотвращения будущих атак:

- •создать новые правила в защитных решениях
- •проверить целостность информации на всех затронутых машинах
- •установить обновления безопасности, чтобы закрыть использованные уязвимости
- установить зараженные узлы, которые требуют восстановления
- •обычно для этого используются индикаторы компрометации
- провести аудит информационной безопасности в системах и сети

Этапы реагирования на инцидент... Устранение

- Восстановите работоспособность системы
- Сохраните чистые, обновленные резервные копии
- Поменяйте пароли в локальной системе и на сетевых ресурсах
- Администратор должен понаблюдать за системой, чтобы убедиться в ее нормальной работе
- Продолжайте тестирование целостности данных в системе
- Документируйте предпринятые шаги
- Восстановление позволяет заново запустить этап локализации при возобновлении вредоносной активности

Этапы реагирования на инцидент...Резюме



Сбор цифровых доказательств

Сбор цифровых доказательств

Подготовка к сбору цифровых доказательств - это важный этап цифрового расследования или инцидентного реагирования. Этот процесс включает в себя несколько ключевых шагов:

- **Составление плана сбора доказательств**:

  Определить цели сбора доказательств и область, которую вы хотите исследовать.

  Составить детальный план, включающий список систем, устройств и ресурсов, которые будут исследованы.

  Разработать методику и порядок действий для сбора и анализа доказательств.

- **Обеспечение цепи доказательств**:

  Уделить особое внимание сохранению целостности доказательств. Использовать методы и инструменты, которые обеспечивают неизменность данных.

  Документировать каждый этап сбора доказательств, начиная с момента их обнаружения.

- **Определение ресурсов и инструментов**:

  Определить, какие инструменты и оборудование вам понадобятся для сбора и анализа данных.

  Обеспечить доступ к необходимым программным средствам для анализа и восстановления данных.

- **Согласование и юридические аспекты**:

  Удостовериться, что соблюдаются все юридические требования и политики организации в отношении сбора и использования цифровых доказательств.

  При необходимости получить необходимые разрешения или согласование с юридическим отделом.

Сбор цифровых доказательств

- **Обучение персонала**:
  Обеспечьте, чтобы сотрудники, участвующие в сборе доказательств, были обучены и компетентны в использовании соответствующих инструментов и методов.
  Подготовьте персонал к соблюдению процедур и стандартов цифрового расследования.
- **Обеспечение защиты и сохранности данных**:
  Уделяйте особое внимание защите данных от изменений, повреждений или несанкционированного доступа.
  Используйте шифрование и другие меры для обеспечения конфиденциальности данных.
- **Планирование и логистика**:
  Планируйте распределение ресурсов и персонала для сбора доказательств.
  Обеспечьте логистическую поддержку, такую как доступ к физическим устройствам и серверам, если это необходимо.
- **Тестирование и верификация**:
  Проверьте, что все инструменты и методы работают правильно и настроены корректно до начала сбора данных.
- **Документация и отчетность**:
  Ведите подробную документацию обо всех этапах подготовки и сбора доказательств.
  Создайте отчет о выполненной работе и обо всех собранных доказательствах.
- Подготовка к сбору цифровых доказательств помогает обеспечить эффективность и законность всего процесса. Она также способствует сохранности и надежности доказательств, что имеет большое значение при расследовании инцидентов и в судебных процессах.

Инструменты для сбора цифровых доказательств

Сбор цифровых доказательств - важный этап в цифровой криминалистике и инцидентном реагировании. Существует множество инструментов и программных средств, которые помогают специалистам по цифровой криминалистике собирать и анализировать цифровые доказательства. Вот некоторые из них:

- **EnCase**: это популярное программное обеспечение для сбора и анализа цифровых доказательств. Оно используется в правоохранительных и юридических организациях.
- **FTK (Forensic Toolkit)**: еще одно популярное программное обеспечение для цифровой криминалистики, которое помогает в сборе и анализе данных с компьютеров и мобильных устройств.
- **Sleuth Kit / Autopsy**: это бесплатное с открытым исходным кодом программное обеспечение для цифровой криминалистики, которое предоставляет инструменты для анализа файловой системы и восстановления данных.

- **X-Ways Forensics**: программа для сбора и анализа цифровых доказательств с богатыми возможностями.
- **Volatility**: инструмент для анализа дампов оперативной памяти. Он позволяет исследователям извлекать информацию о процессах и объектах из памяти.
- **Wireshark**: если вам нужно анализировать сетевой трафик, Wireshark поможет вам захватить и изучить пакеты данных.
- **dd (Data Duplicator)**: эта утилита Unix/Linux используется для создания физических копий дисков или съемных носителей.
- **Bulk Extractor**: инструмент для автоматического извлечения информации о цифровых доказательствах из больших объемов данных, таких как диски и образы дисков.
- **RegRipper**: этот инструмент предназначен для извлечения и анализа реестра Windows.
- **Oxygen Forensic Detective**: этот инструмент предназначен для извлечения и анализа данных с мобильных устройств, включая смартфоны и планшеты.

- **Cellebrite UFED**: используется для извлечения данных с мобильных устройств и обеспечивает поддержку для разных типов устройств и операционных систем.
- **Digital Forensics Framework (DFF)**: это платформа с открытым исходным кодом, предоставляющая инструменты для сбора, анализа и представления цифровых доказательств.

Выбор инструментов зависит от конкретной задачи и контекста расследования. Специалисты по цифровой криминалистике должны быть знакомы с различными инструментами и выбирать наиболее подходящие для конкретной ситуации. Кроме того, важно соблюдать закон и соблюдать процедуры при сборе и анализе цифровых доказательств.