**Учебный курс:**

**Современные технологии извлечения и анализа данных из цифровых устройств**

|  |  |
| --- | --- |
| **Наименование разделов**  **(дисциплин) и тем** | **Содержание обучения (по темам в дидактических единицах)** |
| **Раздел 1. Основы мобильной криминалистики** | |
| Тема 1.1. Мобильные устройства как объект криминалистического исследования: изучаем все аспекты | * Введение в мобильную криминалистику: Определение понятия, его актуальность в современном правоприменении. * Структура мобильного устройства: Элементы архитектуры и функционирования: процессор, память, интерфейсы. * Типы хранимой информации: * Текстовые сообщения: SMS, мессенджеры, их значение и возможности извлечения. * Изображения и видео: источники данных для анализа, форматы и методы извлечения. * Контакты: важность информации о связях, хранение данных в облаке и на устройстве. * Метаданные: понимание и использование метаданных, как способа реконструкции событий. * Формирование полной картины преступления: Как данные помогают восстанавливать хронологию событий и выявлять связи между участниками. |
| Тема 1.2. Обзор ключевых мобильных платформ | * Анализ архитектуры iOS: Общая структура, особенности системы, подходы к безопасности. * Изучение Android: Гибкость системы, разные версии, механизмы защиты данных. * Windows Phone: Характеристика платформы, её уникальные функции и ограничения. * Сравнительный анализ: Достоинства и недостатки каждой платформы с точки зрения криминалистического анализа, включая шифрование и доступ к данным. |
| Тема 1.3. Алгоритм сохранения и извлечения данных | * Этапы извлечения данных: Подробный разбор последовательных действий для проведения исследования, начиная от подготовки до анализа. * Оценка состояния устройства: Как состояние мобильного устройства влияет на процесс извлечения данных и его результаты. * Методы создания образов данных: Используемые технологии для копирования и анализа информации с устройства. * Юридические нормы: Значение соблюдения протоколов и правовых аспектов при извлечении данных для обеспечения их допустимости в судебном разбирательстве. |
| Тема 1.4. Сравнительный анализ физических, логических и облачных методов исследования | * Физические методы: Обзор техник прямого извлечения данных с устройства, их преимущества и недостатки. * Логические методы: Механизмы анализа через программное обеспечение, методы работы с резервными копиями и их использование в расследовании. * Облачные технологии: Применение облачных решений для извлечения данных, возможность взаимодействия с удалёнными серверами, преимущества и риски. * Выбор метода: Условия и ситуации, при которых каждый из методов может быть наиболее эффективным. |
| Тема 1.5. Основные принципы криминалистических исследований мобильных устройств: правила и общий порядок работы | * Этические нормы: Значение этики в криминалистическом исследовании и защите прав граждан. * Протоколы и правила: Основные принципы работы, обеспечивающие качество и допустимость доказательств. * Документация: Формирование отчётов о проведении экспертизы, методах и результатах. * Безопасность исследований: Основные стандарты и протоколы, направленные на защиту данных и сведений, выявленных в ходе работы. |
| Тема 1.6. Инструменты для анализа информации с мобильных устройств | * Обзор программного обеспечения: Сравнение различных программ, используемых в мобильной криминалистике. * Оборудование для низкоуровневого доступа: Специальные устройства и технологии для физического извлечения данных. * Критерии выбора инструментов: Как действовать в зависимости от типа устройства и характера поставленной задачи. |
| Тема 1.7. Техники извлечения данных из мобильных устройств | * Методы программного и аппаратного извлечения: Углубленное изучение различных подходов к работе с данными. * Обход защитных механизмов: Техники преодоления блокировок и средств защиты информации. * Практическое применение: Рекомендации по реализации выработанных методов в условиях реального расследования, анализ реальных примеров. |
| Тема 1.8. Способы получения данных из iOS-устройств с использованием продуктов Elcomsoft | * Инструменты Elcomsoft: Обзор доступных решений для работы с устройствами Apple. * Методы обхода ограничений системы: Практические аспекты работы с паролями |
| **Раздел 2. Низкоуровневое извлечение** | |
| Тема 2.1. Введение в основы низкоуровневого анализа | * Понимание концепций и методов низкоуровневого анализа данных. * Изучение принципов работы с памятью мобильных устройств. * Невозможность полного учета различий между низкоуровневыми и высокоуровневыми методами. |
| Тема 2.2. Механизмы защиты мобильных устройств и техники извлечения данных | * Изучение основных механизмов безопасности мобильных устройств. * Ознакомление с методами шифрования и аутентификации. * Исследование подходов к извлечению данных при наличии защиты. |
| Тема 2.3. Понятие уязвимостей загрузчиков | * Анализ уязвимостей, связанных с загрузчиками мобильных устройств. * Ознакомление с типами загрузчиков и их ролью в безопасности. * Изучение методов эксплуатации уязвимостей для извлечения данных. |
| Тема 2.4. Извлечение данных из iPhone и iPad | * Освоение решений от Elcomsoft для извлечения данных из устройств Apple. * Понимание работы с учетными записями iCloud и резервными копиями. |
| Тема 2.5. Физический анализ и джейлбрейк | * Изучение физических методов анализа, включая джейлбрейк. * Оценка преимуществ и недостатков применения этих методов. |
| Тема 2.6. Установка и использование агента-экстрактора | * Ознакомление с процессом установки и настройки агента-экстрактора. * Понимание работы с инструментами для автоматизации извлечения данных. |
| Тема 2.7. Препятствия при извлечении и расшифровке информации | * Анализ проблем, возникающих при извлечении и расшифровке данных. * Изучение практических аспектов, связанных с шифрованием и физическим повреждением устройств. |
| Тема 2.8. Методы получения данных с устройств Qualcomm | * Освоение методов извлечения данных с устройств на платформе Qualcomm. * Понимание технических аспектов и используемых инструментов. |
| Тема 2.9. Извлечение информации из чипсетов Spreadtrum и МТК | * Изучение техник и инструментов для извлечения данных из чипсетов Spreadtrum и MediaTek. * Ознакомление с особенностями платформ, влияющими на процедуры извлечения. |
| Тема 2.10. Специфика чипов Samsung Exynos | * Анализ архитектуры и механизмов безопасности чипов Samsung Exynos. * Понимание применения методов извлечения данных для этих чипов. |
| **Раздел 3. Низкоуровневое и логическое извлечение** | |
| Тема 3.1. Техники подбора паролей для расшифровки данных | * Углубленное изучение методов подбора паролей, направленных на расшифровку зашифрованных данных. * Исследование теоретических основ и практических навыков, позволяющих эффективно использовать инструменты подбора паролей, включая алгоритмы шифрования и уровни сложности. Особое внимание будет уделено методам перебора, таким как брутфорс и словарные атаки, а также применению специализированного программного обеспечения для оптимизации процесса. |
| Тема 3.2. Способы извлечения данных из поврежденных устройств | * Анализ методов извлечения данных из устройств с физическими или логическими повреждениями. * Обзор причин повреждений — механических и программных — и их влияния на доступность данных. * Описание технологий восстановления данных, включая использование программных и аппаратных решений, а также анализ файловых систем. |
| Тема 3.3. Кросс-платформенные методы извлечения данных | * Изучение кросс-платформенных методов извлечения данных, применяемых к устройствам разных производителей и операционных систем. Углубленное понимание ключевых отличий платформ, таких как iOS и Android, и лучших практик применения универсальных инструментов. Обсуждение техник быстрого доступа к информации, что позволит участникам эффективно справляться с разнообразными условиями работы. |
| **Раздел 4. Основы шифрования и анализа данных в криминалистике** | |
| Тема 4.1. Анализ данных мобильных приложений | * Извлечение информации из приложений для iOS и Android. * Уникальные характеристики и особенности каждой платформы. * Инструменты и методы для глубокого анализа мобильных данных. |
| Тема 4.2. Основы шифрования и его значение в криминалистике | * Введение в виды шифрования. * Влияние шифрования на криминалистику. * Примеры успешного и неудачного анализа зашифрованной информации. |
| Тема 4.3. Возможности восстановления удаленных данных | * Методы восстановления данных с физических носителей. * Технологии восстановления из облачных хранилищ. * Этические и юридические аспекты процесса восстановления. |
| Тема 4.4. Методы доступа к зашифрованной информации | * Способы получения доступа к зашифрованным данным. * Обзор уязвимостей, позволяющих дешифрование. * Правовые рамки и этические нормы, касающиеся доступа к зашифрованной информации. |
| Тема 4.5. Структура Elcomsoft Premium Forensic Bundle | * Обзор функциональности Elcomsoft Premium Forensic Bundle. * Интерактивная демонстрация инструментов и возможностей. * Применение программного обеспечения в практике криминалистики. |
| Тема 4.6. Основные действия при извлечении информации с цифровых носителей с целью их исследования | * Основные этапы извлечения информации из цифровых носителей. * Методы сохранения целостности данных и эффективного сбора доказательств. * Рекомендации при извлечении информации с цифровых носителей |
| **Раздел 5. Облачные технологии в криминалистике** | |
| Тема 5.1. Роль облачных сервисов в мобильной криминалистике | * Влияние облачных технологий на современную криминалистику * Преимущества облачных платформ для хранения данных * Возможности обработки данных и анализа улик * Новейшие методы расследования, основанные на облачных сервисах |
| Тема 5.2. Извлечение данных из облаков iCloud и Google Account | * Обзор типов данных, извлекаемых из iCloud и Google Account * Подробные методы извлечения информации * Инструменты для эффективного извлечения данных * Практические примеры успешного извлечения информации |
| Тема 5.3. Основы аутентификации и двухфакторной авторизации | * Принципы аутентификации в контексте облачных технологий * Значение двухфакторной авторизации для защиты учетных записей * Разнообразие методов аутентификации |
| Тема 5.4. Роль токенов безопасности и маркеров аутентификации | * Определение токенов безопасности и маркеров аутентификации * Влияние токенов на извлечение данных из облачных сервисов * Значимость токенов для обеспечения безопасности * Практические аспекты использования токенов в криминалистике |
| Тема 5.5. Уникальные аспекты защиты с использованием двухфакторной аутентификации | * Особенности двухфакторной аутентификации как механизма защиты * Общие угрозы, связанные с 2FA * Рекомендуемые практики для повышения уровня безопасности * Анализ успешных случаев применения двухфакторной аутентификации |
| Тема 5.6. Извлечение паролей от учетных записей и данных приложений | * Методы извлечения паролей из различных источников * Инструменты для осуществления извлечения с учетом юридических норм * Этические аспекты извлечения данных * Обсуждение кейсов и успешных практик в данной области |
| Тема 5.7. Доступ к данным мессенджеров через облачные сервисы | * Обзор методов получения данных из мессенджеров * Меры безопасности, используемые в мессенджерах * Инструменты для извлечения информации из мессенджеров * Актуальные примеры и технологии, обеспечивающие доступ к данным |
| Тема 5.8. Получение информации из социальных сетей | * Техники и инструменты для извлечения данных из социальных сетей * Методы анализа собранной информации * Этические и юридические аспекты работы с данными из социальных сетей * Примеры использования данных из социальных сетей в криминалистике |