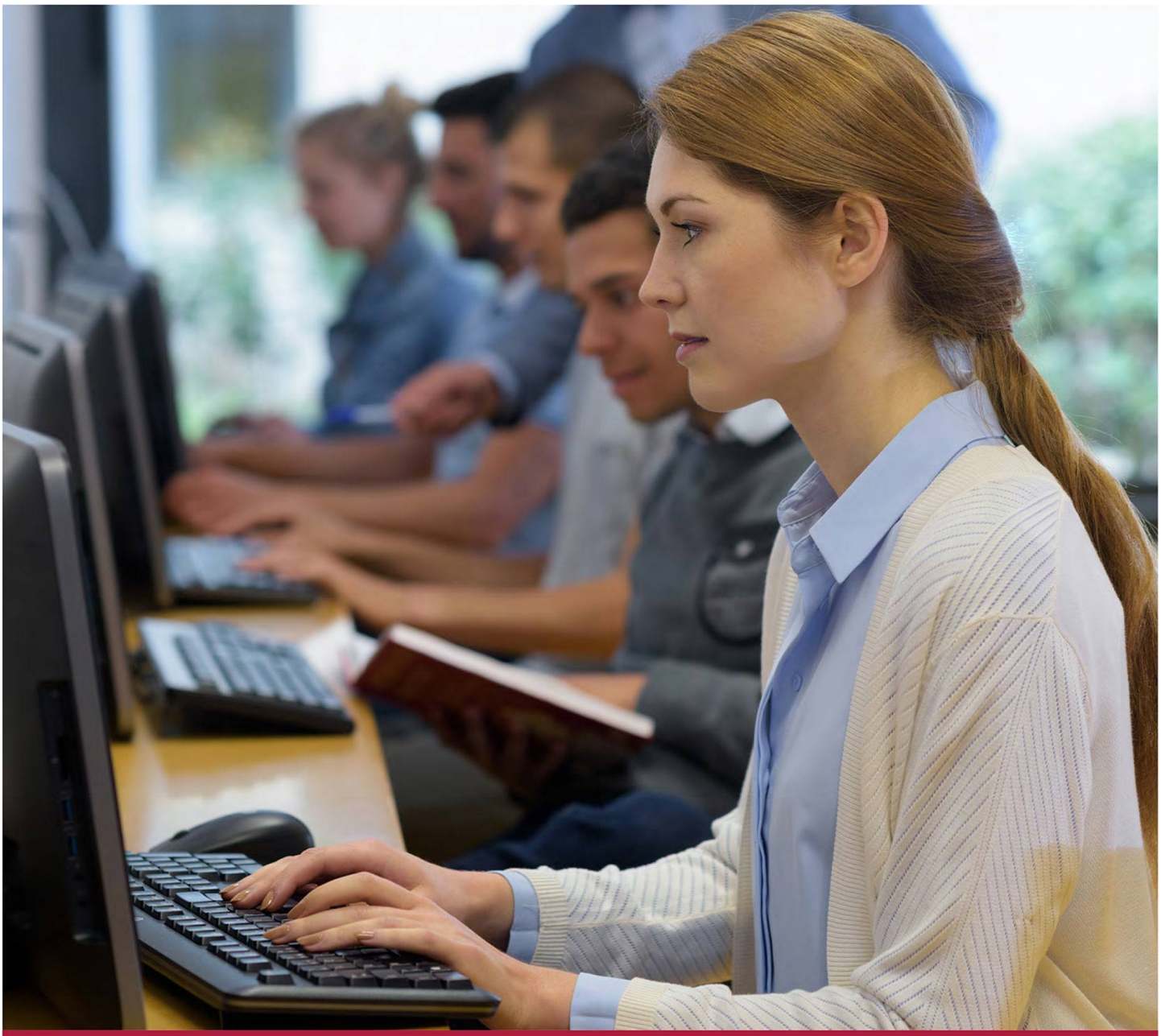
Академия АйТи
a Softline Company



Расследования компьютерных инцидентов. Компьютерная криминалистика

Код курса: ИБ044

+7 (495) 150 96 00 | academy@academyit.ru | academyit.ru

Расследования компьютерных инцидентов. Компьютерная криминалистика

Код курса: ИБ044

Длительность	40 ак. часов
Формат	
Разработчик курса	Академия АйТи
Тип	Учебный курс
Способ обучения	Под руководством тренера

О курсе

В курсе рассматриваются основные приемы и методы компьютерной криминалистики – форензик. Форензика - раскрытие преступлений, связанных с компьютерной информацией, исследование цифровых доказательств, методы поиска, получения и закрепления таких доказательств. В ходе изучения курса слушатели приобретут навыки поиска цифровых следов в компьютерных системах, фиксации этих следов, анализа собранных материалов с целью выявления источника атаки и восстановления работоспособности системы, навыки подготовки отчета по расследованиям инцидента. На курсе будут рассмотрены инструменты для проведения криминалистического анализа и сбора цифровых доказательств, методы и средства по реагированию на инциденты информационной безопасности, техники, затрудняющие криминалистическую экспертизу, психологические особенности расследования преступления

Подробная информация

Успешное окончание обучения по программе данного курса позволит специалистам:

Определить место компьютерной криминалистики в современном мире

Применять программные средства, необходимые в процессе криминалистического расследования

Расследовать компьютерные инциденты

Обозначить структуру жесткого диска и файловых систем, проводить анализ файловых систем

Применять программные средства для извлечения данных с жестких дисков

Применять программные средства для взлома паролей приложений

Составлять отчет о расследовании инцидента

Цель курса

Формирование знаний и навыков, необходимых для извлечения и анализа данных из операционных систем с использованием различных инструментов и подходов.

Программа курса

Модуль 1. Компьютерная криминалистика в современном мире

Что такое компьютерная криминалистика и ее применение

Виды компьютерных преступлений

Разбор кейсов — примеры расследования компьютерных преступлений

Сложности криминалистической экспертизы

Расследование киберпреступлений (гражданское, уголовное, административное)

Нормативные правовые акты в области информационных технологий и защиты информации

Уголовно-правовая характеристика компьютерных преступлений

Криминалистическая характеристика компьютерных преступлений

Ответственность за нарушения требований законодательства

Правила судебно-медицинской экспертизы

Расследование преступлений, совершенных организованными преступными группами (Enterprise Theory of Investigation)

Цифровые улики и их типы

Характеристики цифровых улик

Роль цифровых улик

Источники потенциальных улик

Правила сбора доказательств

Требование представления наилучших доказательств

Кодекс доказательственного права

Производные доказательства

Научная рабочая группа по цифровым уликам (SWGDE)

Готовность к криминалистическому расследованию

Компьютерная криминалистика как часть плана реагирования на инциденты

Необходимость компьютерной криминалистики

Роли и обязанности следователя судебной экспертизы

Проблемы криминалистического расследования

Правила этики

Ресурсы по компьютерной криминалистике

Лабораторная работа: Подготовка лаборатории для практических экспериментов

Лабораторная работа: Изучение основ расследования компьютерных преступлений

Модуль 2. Процесс расследования компьютерных инцидентов

Важность процесса расследования

Фазы процесса расследования

Этап предварительного расследования

Подготовка криминалистической лаборатории

Построение следственной группы

Обзор политик и законов

Создание процессов обеспечения качества

Знакомство со стандартами уничтожения данных

Следственные и процессуальные действия

Особенности осмотра места происшествия

Оценка риска и оперативное реагирование

Досмотр и изъятие

Проведение предварительных интервью

Особенности проведения выемки носителей информации

Ордер на обыск и изъятие

Работа с включенными компьютерами

Работа с выключенными компьютерами

Работа с сетевым компьютером

Работа с открытыми файлами и файлами автозагрузки

Процедура выключения операционной системы

Работа с рабочими станциями и серверами

Работа с портативными компьютерами

Работа с включенными портативными компьютерами

Защита и управление уликами

Сбор и восстановление данных

Анализ данных и программное обеспечение анализа данных

Этап после расследования

Оценка улик и найденных доказательств

Документация и отчетность

Документация по каждой фазе расследования

Сбор и упорядочивание информации

Написание отчета об исследовании

Экспертное свидетельствование

Лабораторная работа: Изучение и практическое применение программных средств, необходимых в процессе криминалистического расследования

Модуль 3. Жесткие диски и файловые системы

Обзор жестких дисков

Жесткие диски (HDD)

Твердотельные накопители (SSD)

Физическая структура жесткого диска

Логическая структура жесткого диска

Типы интерфейсов жестких дисков

Интерфейсы жестких дисков

Треки

Секторы

Кластеры

Плохие секторы

Бит, байт и полубайт

Адресация данных на жестком диске

Плотность данных на жестком диске

Расчет емкости диска

Измерение производительности жесткого диска

Разделы диска и процесс загрузки

Дисковые разделы

Блок параметров BIOS

Главная загрузочная запись (MBR)

Глобальный уникальный идентификатор (GUID)

Что такое процесс загрузки?

Основные системные файлы Windows

Процесс загрузки Windows

Идентификация таблицы разделов GUID

Анализ заголовка и записей GPT

Артефакты GPT

Процесс загрузки Linux

Файловые системы

Общие сведения о файловых системах

Типы файловых систем

Файловые системы Windows

Файловые системы Linux

Виртуальная файловая система (VFS)

Система хранения RAID

Уровни RAID

Защищенные области хоста (HPA)

Анализ файловой системы

Выделение однородных массивов данных

Анализ файла изображения (JPEG, BMP, шестнадцатеричный вид форматов файлов изображений)

Анализ файла PDF

Анализ файлов Word

Анализ файлов PPT

Анализ фалов Excel

Шестнадцатеричный вид популярных форматов файлов (видео, аудио)

Анализ файловой системы

Лабораторная работа: Восстановление удаленных файлов

Лабораторная работа: Анализ файловых систем

Модуль 4. Сбор и дублирование данных

Концепции сбора и дублирования данных, типы систем сбора данных

Получение данных в реальном времени

Порядок волатильности

Типичные ошибки при сборе изменчивых данных

Методология сбора изменчивых данных

Получение статических данных

Статические данные

Эмпирические правила

Дубликаты образов

Побитовая копия и резервная копия

Проблемы с копированием данных

Шаги по сбору и дублированию данных

Подготовка формы передачи улик

Включение защиты от записи на носителях-уликах

Подготовка целевого носителя: руководство NIST SP 800-88

Определение формата сбора данных

Методы сбора данных

Определение лучшего метода сбора данных

Выбор инструмента для сбора данных

Сбор данных с RAID-дисков

Удаленное получение данных

Ошибки при сборе данных

Планирование нештатных ситуаций

Рекомендации по сбору данных

Поиск цифровых артефактов (следов) компрометации штатными средствами ОС Windows, Linux

Сбор данных с web-серверов

Лабораторная работа: Применение программных средств для извлечения данных с жестких дисков

Модуль 5. Техники, затрудняющие криминалистическую экспертизу

Что такое антифорензика и ее цели

Техники антифорензики

Удаление данных / файлов, что происходит при удалении файла в Windows

Восстановление файлов

Средства восстановления файлов в Windows

Восстановление файлов в Linux

Восстановление удаленных разделов

Защита паролем

Типы паролей

Работа взломщика паролей

Техники взлома паролей

Пароли по умолчанию

Использование радужных таблиц для взлома хэшей

Аутентификация Microsoft

Взлом системных паролей

Обход паролей BIOS

Инструменты для сброса пароля администратора, паролей приложений, системных паролей

Стеганография и стеганализ

Скрытие данных в структурах файловой системы

Обфускация следов

Стирание артефактов

Перезапись данных и метаданных

Шифрование

Шифрующая файловая система (EFS)

Инструменты восстановления данных EFS

Шифрованные сетевые протоколы

Упаковщики

Руткиты, шаги для их обнаружения

Минимизация следов

Эксплуатация ошибок криминалистических инструментов

Детектирование криминалистических инструментов

Меры противодействия антифорензике

Инструменты, затрудняющие криминалистическую экспертизу

Лабораторная работа: Применение программных средств для взлома паролей приложений

Лабораторная работа: Обнаружение стеганографии

Модуль 6. Подготовка отчета о расследовании

Подготовка отчета об исследовании

Показания эксперта-свидетеля

Свидетельство в суде

Показания, приобщенные к материалам дела

Работа со СМИ

Разработка документов, необходимых для проведения расследования компьютерных инцидентов

Разработка Частной политики управления инцидентами

Разработка Регламента расследования

Проведение расследования компьютерного инцидента

Взаимодействие с правоохранительными органами, специализированными организациями и представительство интересов организации в суде

Практическая работа: Проведение расследования компьютерного инцидента.

Модуль 7. Психологические особенности расследования компьютерных инцидентов

Психологический анализ личности преступника.

Особенности формирования преступной мотивации.

Системы DLP.

Выявление и расследование корпоративного мошенничества.

Расследование утечек информации.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

+7 (495) 150 96 00 | academy@academyit.ru