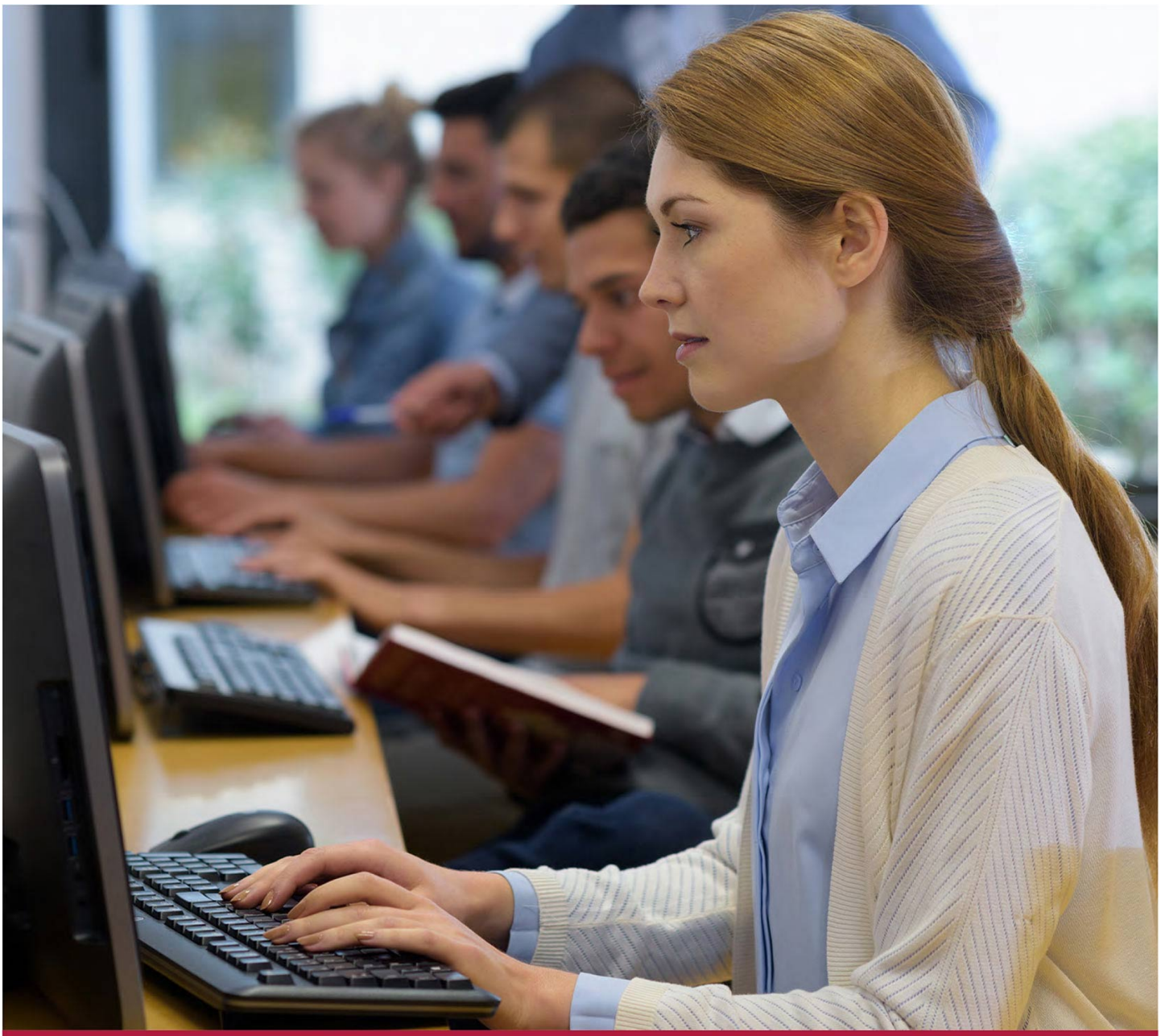
Академия АйТи
a Softline Company



Компьютерная криминалистика операционных систем. Windows/Linux

Код курса: ИБ045

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

Компьютерная криминалистика операционных систем. Windows/Linux

Код курса: ИБ045

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

О курсе

Форензика - компьютерная криминалистика, расследование киберпреступлений, связанных с компьютерной информацией. Сегодня компаниям нужны специалисты в области форензики в Windows / Linux, имеющие знания и навыки проведения компьютерной экспертизы и владеющие современными технологиями кибераразведки. Эксперты по компьютерной криминалистике сочетают в себе навыки программиста, аналитика данных и следователя.

Подробная информация

Успешное окончание обучения по программе данного курса позволит специалистам:

Проводить криминалистическую экспертизу операционных систем

Исследовать сетевой трафик

Расследовать атаки на сервер

Расследовать зловредное программное обеспечение

Готовить отчет о расследовании

Необходимая подготовка

Базовые знание компьютерной криминалистики

Знание ОС Windows

Цель курса

Формирование знаний и навыков, необходимых для извлечения и анализа данных из операционных

систем персональных компьютеров с использованием различных инструментов и подходов

Программа курса

Модуль 1. Криминалистическая экспертиза операционных систем

Введение в криминалистическую экспертизу ОС

Криминалистическая экспертиза Windows

Методология криминалистической экспертизы Windows

Сбор энергозависимой информации (системное время, зарегистрированные пользователи, открытые файлы, информация о сети, сетевые подключения, информация о процессах, сопоставление процессов и портов, память процесса, состояние сети, файлы очереди печати и др.)

Сбор энергонезависимой информации (файловые системы, настройки реестра, идентификаторы безопасности (SID), журналы событий, файл базы данных ESE, подключенные устройства, файлы гибернации, файл подкачки, скрытые альтернативные потоки и др.)

Анализ памяти Windows (виртуальные жесткие диски (VHD), дамп памяти, механизм создания процесса, анализ содержимого памяти, анализ памяти процесса, извлечение образа процесса, сбор содержимого из памяти процесса)

Анализ реестра Windows (устройство реестра, структура реестра, реестр как файл журнала, анализ реестра, системная информация, информация о часовом поясе, общие папки, беспроводные идентификаторы SSID, служба теневого копирования томов, загрузка системы, вход пользователя, активность пользователя, ключи реестра автозагрузки, USB-устройства, монтируемые устройства, отслеживание активности пользователей, ключи UserAssist)

Кэш, Cookie и анализ истории (Mozilla Firefox, Google Chrome, Microsoft Edge и Internet Explorer)

Анализ файлов Windows (точки восстановления системы, Prefetch-файлы, ярлыки, файлы изображений)

Исследование метаданных (типы метаданных, метаданные в разных файловых системах, метаданные в файлах PDF, метаданные в документах Word, инструменты анализа метаданных)

Журналы (типы событий входа в систему, формат файла журнала событий, организация записей событий, структура ELF_LOGFILE_HEADER, структура записи журнала, журналы событий Windows 10, криминалистический анализ журналов событий)

Инструменты криминалистического анализа Windows

Криминалистическая экспертиза LINUX

Команды оболочки

Файлы журнала Linux

Сбор энергозависимых данных

Сбор энергонезависимых данных

Область подкачки

Лабораторная работа: Обнаружение и извлечение материалов для анализа

Лабораторная работа: Извлечение информации о запущенных процессах

Лабораторная работа: Анализ событий

Лабораторная работа: Выполнение криминалистического исследования

Лабораторная работа: Сбор и анализ энергозависимых данных в Linux

Модуль 2. Сетевые расследования, логи и дампы сетевого трафика

Введение в сетевую криминалистику (анализ по журналам и в реальном времени, сетевые уязвимости, сетевые атаки)

Основные понятия ведения журналов (лог-файлы как доказательство, законы и нормативные акты, законность использования журналов, записи о регулярно проводимой деятельности в качестве доказательства)

Корреляция событий

Типы корреляции событий

Пререквизиты для корреляции событий

Подходы к корреляции событий

Обеспечение точности лог-файлов

Запись

Сохранение времени

Цель синхронизации времени компьютеров

Протокол сетевого времени (NTP)

Использование нескольких датчиков

Управления журналами

Функции инфраструктуры управления журналами

Проблемы с управлением журналами

Решение задач управления журналами

Централизованное ведение журнала

Протокол Syslog

Обеспечение целостности системы

Контроль доступа к журналам

Цифровая подпись, шифрование и контрольные суммы

Анализ журналов

Механизм сетевого криминалистического анализа

Средства сбора и анализа журналов

Анализ журналов маршрутизатора

Сбор информации из таблицы ARP

Анализ журналов брандмауэра, IDS, Honeypot, DHCP, ODBC

Исследование сетевого трафика

Сбор улик посредством сниффинга

Анализаторы сетевых пакетов

Документирование сетевых улик

Реконструкция улик

Модуль 3. Расследование зловредного программного обеспечения

Концепции и типы вредоносного ПО

Различные способы проникновения вредоносного ПО в систему

Методы, используемые злоумышленниками для распространения вредоносного ПО в интернете

Компоненты вредоносного ПО

Криминалистическая экспертиза вредоносных программ

Анализ вредоносного ПО

Идентификация и извлечение вредоносных программ

Лаборатория для анализа вредоносных программ

Подготовка тестового стенда для анализа вредоносных программ

Инструменты для анализа вредоносных программ

Общие правила анализа вредоносных программ

Организационные вопросы анализа вредоносных программ

Типы анализа вредоносных программ

Статический анализ

Статический анализ вредоносных программ: отпечатки файлов

Онлайн-службы анализа вредоносных программ

Локальное и сетевое сканирование вредоносных программ

Выполнение поиска строк

Определение методов упаковки / обфускации

Поиск информации о переносимых исполняемых файлах (PE)

Определение зависимостей файлов

Дизассемблирование вредоносных программ

Средства анализа вредоносных программ

Динамический анализ

Мониторинг процессов, файлов и папок, реестра, активности сети, портов, DNS, вызовов API, драйверов устройств, программ автозагрузки, служб Windows

Анализ вредоносных документов

Проблемы анализа вредоносных программ

Модуль 4. Подготовка отчета о расследовании

Подготовка отчета об исследовании

Классификация отчетов

Руководство по написанию отчета

Рекомендации по написанию отчета

Показания эксперта-свидетеля

Роль эксперта-свидетеля

Технический свидетель и эксперт-свидетель

Стандарт Дьюберта

Стандарт Фрайе

Правила хорошего эксперта-свидетеля

Важность резюме

Профессиональный кодекс свидетеля-эксперта

Подготовка к даче свидетельских показаний

Свидетельство в суде

Общий порядок судебных разбирательств

Общая этика при свидетельстве

Значение графики в показаниях

Как избежать проблем с показаниями

Свидетельствование во время прямой экспертизы

Свидетельствование во время перекрестного допроса

Показания, приобщенные к материалам дела

Работа со СМИ

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Академии АйТи

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