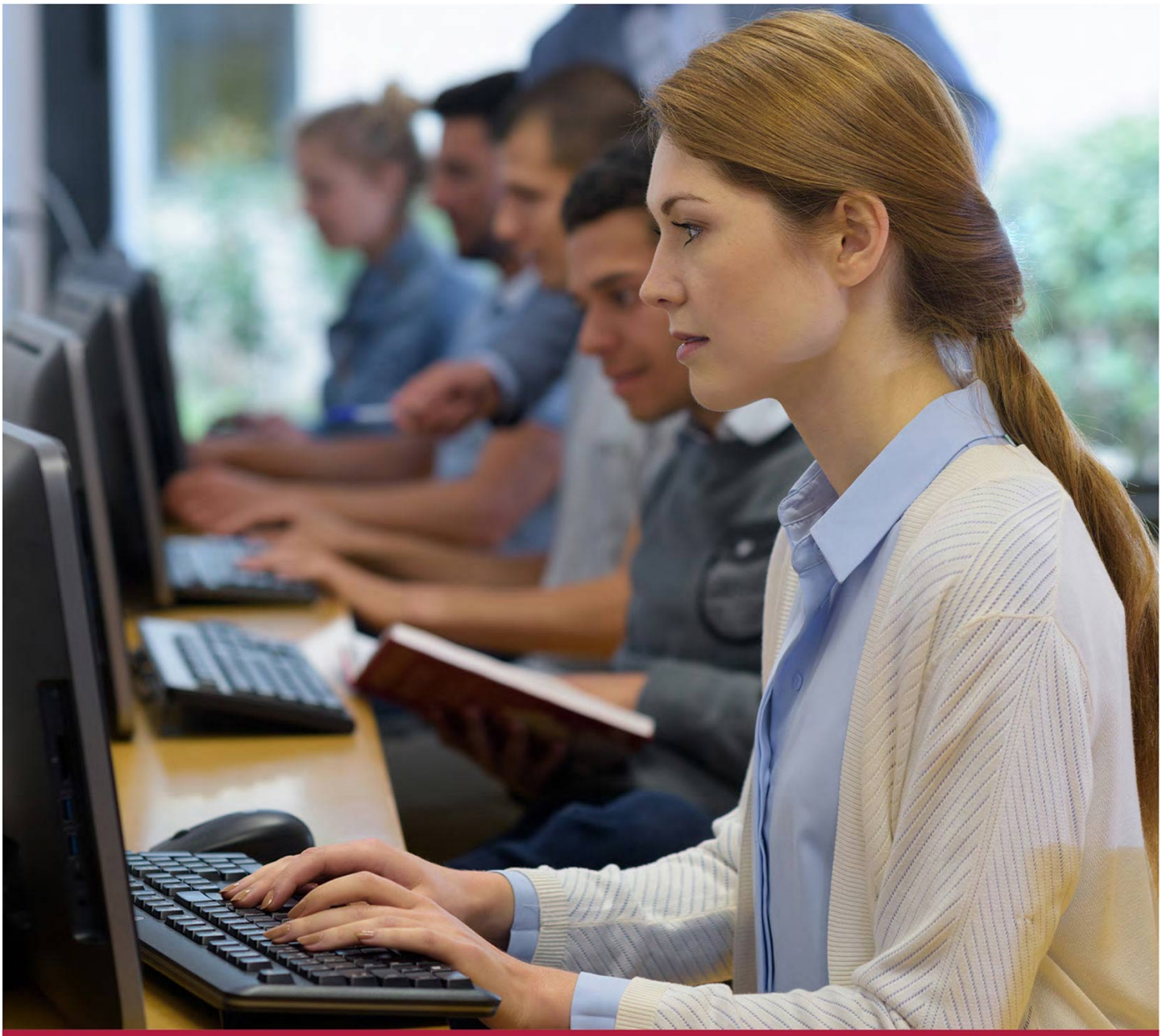
softline®

Учебный центр Softline



Цифровая криминалистика

Код курса: KL-DFKU

8 (800) 505-05-07 | edusales@softline.com | edu.softline.com

Цифровая криминалистика

Код курса: KL-DFKU

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

О курсе

В данном курсе рассматриваются основные принципы цифровой криминалистики. Данный курс сфокусирован на расследовании инцидентов. Слушатели научатся работать с такими утилитами, как Live Response Tools (Sysinternals), Forensics Live CDs (Helix, Deft), Forensics Disk Imaging (FTK, dd, HDD). Все перечисленные утилиты активно используются в ходе выполнения лабораторных работ. Инструменты меняются со временем, но принципы и методы остаются неизменными. Слушатели научатся не только использовать соответствующие инструменты, но и получат знания фундаментальных принципов цифровой криминалистики. Все практические задания в курсе основаны на реальных случаях. Данный курс проводит Kaspersky Lab, привлекая собственных тренеров (только очно, г. Москва)

Подробная информация

Профиль аудитории:

- Системные и сетевые инженеры, администраторы и специалисты в области сетевой безопасности, архитекторы безопасности.

Предварительные требования:

- Продвинутые навыки системного администрирования.

По окончании курса слушатели смогут:

- Знать основные принципы и методы цифровой криминалистики;
- Выбирать соответствующий инструментарий для расследования инцидентов;
- Работать с реестром Windows при расследовании;
- Анализировать остаточные следы после атаки;
- Анализировать данные в браузерах и клиентах электронной почты.

Программа курса

День 1

Успехи в цифровой криминалистике связаны с эффективным реагированием на инциденты. В следующих темах будут рассмотрены шаги, которые надо предпринять в расследовании и инструменты, которые широко используются для сбора улик в оперативной памяти, на жестком диске при включенной или выключенной системе и связанных с монтированием и чтением образов в Windows или Linux системах.

Такого рода анализ постоянно развивается и является рекомендованным в тех ситуациях, когда анализ должен быть проведен немедленно. В течение первого дня будут продемонстрированы некоторые техники быстрого (live) реагирования с использованием различного набора инструментов.

Слушатели также получат знания из области цифровой криминалистики, включающие в себя знания определений, процессов и процедур. Создание рабочей среды для расследования не тривиальный процесс, так как существует риск потери данных, сбоя оборудования и даже заражения системы, вызванное в процессе расследования. В последующих модулях будут даны рекомендации по настройке рабочей станции для расследования, будут рассмотрены преимущества виртуализации в создании мультиплатформенной среды для запуска различных утилит.

Отличия между HDD и SSD дисками делают невозможность использовать те же процедуры при анализе, поэтому в курсе рассматриваются отличия SSD-дисков и сложности, связанные анализом данных на таких дисках.

Модуль 1 Введение в цифровую криминалистику

- Общие термины и принципы
- Процедуры и процессы
- Создание лабораторной среды
- Виртуализация

Модуль 2 Расследования инцидентов и сбор улик

- Основы расследования инцидентов
- Тестовый сценарий
- Анализ оперативной памяти
- Live Response Tools (Sysinternals)
- Forensics Live CDs (Helix, Deft)
- Удаленный анализ
- Forensics Disk Imaging (FTK, dd, HDD)
- SSD и цифровая криминалистика
- Монтирование образов в Windows и Linux (FTK, mount)

День 2

Реестр является одним из важнейших источников для сбора данных в Windows-системах и обязательным для анализа в цифровой криминалистике. Используя реестр, исследователь может извлечь важную информацию об операционной системе, такую как временная зона, сетевой адрес,

посещенные вебсайты, политика безопасности и автоматически запускаемые программы. Пользовательская активность, такая как регистрация в системе или открытые файлы также может быть извлечена из реестра. Вредоносное ПО обычно создает записи в реестре для того, чтобы можно было продолжить работать после перезагрузки или выходы пользователя из системы. Это может дать исследователю необходимые для расследования улики.

В данном модуле рассматривается структура реестра и расположение различных ветвей реестра в файловой системе. Слушатели научатся навигации по ветвям реестра онлайн или офлайн, извлекая файлы реестра из образа системы.

Модуль 3 Анализ реестра Windows

- Структура реестра
- Извлечение пользовательских ветвей реестра
- Данные профиля пользователя
- Доказательная информация в реестре
- Восстановление реестра Windows
- Анализ пользовательской и системной активностей

День 3

Операционная система Windows использует различные файловые структуры и форматы для хранения данных об операциях. Также как и реестр, некоторые файлы представляют интерес для исследователя. Извлеченная информация может помочь в расследовании, поэтому понимание структуры этих файлов является крайне важным. В данном модуле рассматривается нахождение и просмотр файлов журнала событий, файлов .lnk, задач Windows, файлов prefetch и содержимого Корзины. В модуле также рассматривается извлечение информации из связанных файлов, таких как данные exif, файлы MS Office, эскизов изображений (thumbnails).

Модуль 4 Анализ остаточных следов (артефактов) в Windows

- Анализ артефактов в Windows
- Prefetch (WinPrefetchView)
- Журналы событий
- LNK
- Jobs
- Корзина
- Метаданные связанных файлов (EXIF, Thumbnails, файлы Office)

День 4

Во время веб-серфинга важная информация сохраняется в файловой системе. Структура и расположение этой информации отличается для разных браузеров. В Модуле 5 будет рассмотрено, как находить и анализировать историю браузеров, файлы кэша, закладки, файлы cookies и др. Рассматриваются все популярные браузеры.

Электронная почта является стандартным методом для рабочих и личных коммуникаций. Файлы электронной почты содержат важную информацию для расследования. Так как существуют различные системы электронной почты, то исследователь должен понимать принципы работы различных почтовых клиентов, находить, анализировать и извлекать информацию из

соответствующих файлов. В Модуле 6 рассматривается использование веб-клиентов электронной почты, а также почтовые клиенты Outlook и Lotus Notes.

Модуль 5 Исследование браузеров

- Расположение данных в различных браузерах
- Анализ IE
- Анализ Chrome
- Анализ Firefox

Модуль 6 Исследование электронной почты

- Структура клиент-сервер
- Исследование Outlook
- Lotus Notes
- Почтовые web-клиенты

День 5

В последний день курса слушатели выполнят несколько заданий, которые позволят проверить знания и навыки, полученные на курсе. Слушатели изучат несколько различных типов файлов, к которым они должны применить методы цифровой криминалистики. Результаты и выводы слушателей затем будут рассмотрены всей группой.

Полученные навыки

- Умение собирать и анализировать цифровые следы/улики;
- Во время курса слушатели выполнят реконструкцию инцидента с использованием штампов времени и найдут следы вторжения в исследуемые компоненты операционной системы Windows;

Операционная система сама по себе только один из источников получения информации. Слушатели также научатся анализировать историю браузеров и электронной почты и использовать соответствующие программы для извлечения данной информации.

Посмотреть расписание курса и записаться на обучение

Обращайтесь по любым вопросам
к менеджерам Учебного центра Softline

8 (800) 505-05-07 | edusales@softline.com

Ждём вас на занятиях в Учебном центре Softline!

Почему Учебный центр Softline?

Лидер на рынке корпоративного обучения.

Более 300 тысяч подготовленных IT-специалистов.

Гибкий индивидуальный подход в обучении, скидки и акции.

Широкая сеть представительств в крупнейших городах РФ и СНГ; дистанционный формат обучение на вашей территории или в арендованном классе в любой точке мира.

Высокотехнологичное оборудование

Более **17 лет** опыта работы

Международные сертификаты для IT-специалистов и пользователей в Центрах тестирования

Сертифицированные тренеры с богатым практическим опытом работы

Авторизации от мировых производителей ПО (Microsoft, Cisco, VMware, Citrix, Лаборатория Касперсокого, Oracle, Autodesk, Код безопасности и других).

Разработка курсов и тестов под заказ, внедрение корпоративных систем обучения.

Подробнее об Учебном центре Softline
Вы можете узнать из профайла и презентации