Análise avançada de smartphone da Cellebrite (CASA)

Treinamento forense global

Nível
Especialista

Duração
Quatro dias (28 horas)

Público-alvo
Equipes de perícia

Modo de apresentação
Treinamento conduzido por instrutor

Descrição do curso

Este curso de análise avançada, com duração de quatro dias, investiga detalhadamente e de forma prática a recuperação forense de dados de aplicativos encontrados nos smartphones atuais. Esta aula é recomendada para pessoas familiarizadas com o UFED Physical Analyzer ou que tenham concluído o curso de CCPA. Neste curso, os participantes aprenderão a decodificar informações que não são decodificadas por ferramentas forenses. Eles também utilizarão softwares de terceiros e scripts Python para analisar, verificar e validar as descobertas.

Módulo	Descrição e objetivos
Estruturas de bases de dados SQLite	Este módulo é voltado para as estruturas e funcionalidades das bases de dados SQLite. Você aprenderá sobre arquivos de registro e memória compartilhada de gravação antecipada, manuseio de objetos binários grandes, listas e manuseio de páginas livres, função de vácuo e como ocorre a junção dos dados da tabela. Você fará exercícios práticos usando o UFED Physical Analyzer e verificará suas descobertas usando outras ferramentas de software e será capaz de: • Identificar o hardware do dispositivo móvel. • Identificar bases de dados SQLite. • Identificar estruturas de bases de dados SQLite. • Explicar como os dados são armazenados em bases de dados SQLite. • Explicar como é feita a junção das tabelas SQLite. • Discutir o que acontece quando os dados são excluídos de uma base de dados SQLite e a recuperação de dados. • Alistar funções que podem destruir dados. • Usar scripts para extrair e analisar dados de objetos binários grandes (BLOB) a partir de bases de dados. • Montar aplicativos novos e não suportados usando o SQLite Wizard.
Visão geral e análise do iOS	Neste módulo, você aprenderá sobre a demografia do iOS. Aprenderá o que acontece durante o processo de extração de um dispositivo iOS usando a tecnologia UFED. Mostraremos como os aplicativos são armazenados e acessados, bem como várias maneiras de decodificar informações encontradas em arquivos XML e plist binários. Você também aprenderá sobre esquemas de codificação de data e hora e, usando diversos exercícios práticos, examinará vários arquivos de interesse. Após a conclusão deste módulo, você será capaz de: • Fornecer uma breve visão geral da demografia do iOS. • Identificar dispositivos iOS. • Descrever a estrutura do sistema de arquivos do iOS. • Discutir o suporte a UFED da Cellebrite para análise de iOS. • Analisar as extrações do iOS com o UFED Physical Analyzer. • Identificar e decodificar dados armazenados em base64 a partir de arquivos plist binários. • Analisar vários artefatos, como dados de integridade, uso de dados e arquivos de preferências, para apoiar e usar em suas investigações. • Revisar um aplicativo processado em busca de dados relevantes adicionais. • Analisar um aplicativo não suportado usando o SQLite Wizard e incorporar os dados no Physical Analyzer. • Usar Python para obter dados adicionais do Safari e Webkit e ajudar nas investigações na web. • Detectar novos artefatos a partir de extrações completas do sistema de arquivos, como os de Cellebrite Services e Gray Key.
Acesso a dispositivo iOS	Neste módulo, você aprenderá sobre os desafios causados pela API de proteção de dados encontrada em dispositivos Apple iOS. Aprenderá sobre: • Identificação de hardware do dispositivo iOS • Senhas no iOS • Touch ID – prazos e implicações para a investigação • Recuperação de senhas simples e complexas • Vários métodos para talvez obter acesso a dispositivos iOS bloqueados
Backups de iOS e iCloud	Neste módulo, aprenderemos sobre os backups do iOS encontrados em sistemas de computador, extrações criptografadas do iOS e que tipo de informação pode estar contida neles. Também discutiremos a criptografia e a descriptografia de arquivos de backup usando ferramentas de software livre, backups do iCloud e decodificação. Após a conclusão deste módulo, você será capaz de: • Identificar onde podem ser encontrados os backups do iOS. • Identificar as estruturas de pastas de backup do iOS. • Entender como lidar com backups e extrações criptografados do iOS. • Obter arquivos de backup do iCloud e saber como o Physical Analyzer lida com eles. • Usar software livre para descobrir a senha de um backup criptografado. • Aprender a usar as configurações do iOS para talvez remover a senha de backup.

Módulo	Descrição e objetivos
Visão geral do Android	Neste módulo, discutiremos a evolução do sistema operacional Android desde o seu lançamento em 2007. Você também aprenderá sobre os diferentes sistemas de arquivos normalmente usados e como os dados são armazenados em dispositivos Android e cartões SD. Discutiremos criptografia, extrações e limitações. Após a conclusão deste módulo, você será capaz de: • Explicar brevemente a evolução do sistema operacional Android desde seu lançamento em 2007. • Identificar os diferentes sistemas de arquivos que costumam ser usados por dispositivos Android. • Alistar os dispositivos Android, sistemas de arquivos e aplicativos suportados pela Série UFED da Cellebrite. • Entender os vários métodos de extração de dispositivos Android. • Entender os vários tipos de criptografia do Android e as possíveis maneiras de ignorá-los.
Artefatos do sistema Android	Neste módulo, você aprenderá sobre importantes artefatos do sistema Android. Você aprenderá sobre como obter dados que documentam redes sem fio, configurações de fuso horário, sistemas de arquivos montados, uso de cartão SD, códigos de bloqueio por padrão, informações de Bluetooth e versões de sistema operacional. Essas informações podem ser vitais para a investigação. Após a conclusão deste módulo, você será capaz de: • Discutir como determinar quais sistemas de arquivos foram montados em um dispositivo Android. • Localizar e analisar os logs relevantes do sistema, artefatos do Android e arquivos de dispositivo. • Discutir os esquemas de particionamento usados em dispositivos Android. • Analisar outros aplicativos que podem ser valiosos para uma investigação. • Localizar e decodificar logs de uso de aplicativos. • Identificar e analisar dados de arquivos de contas de usuário do Android.
Artefatos do usuário Android	Neste módulo, você aprenderá sobre artefatos criados pela interação do usuário com diferentes aplicativos no dispositivo Android. Usando exercícios práticos, você examinará: Dados do Google Maps, aplicativos não suportados e artefatos que armazenam dados sobre a atividade do usuário que não são analisados como parte de qualquer extração de ferramenta. Após a conclusão deste módulo, você será capaz de: • Decodificar registros de chamadas e registros de data e hora. • Rastrear o movimento de arquivos transferidos por download dentro de um dispositivo Android. • Identificar a localização das mídias. • Interpretar contas de armazenamento baseadas na nuvem usadas em um dispositivo móvel. • Decodificar informações relacionadas a aplicativos que não são decodificados automaticamente por nenhuma ferramenta forense. • Usar scripts Python para ajudar na decodificação de dados. • Localizar dados de itens de dados de usuário relevantes a partir de aplicativos suportados e não suportados usados em um dispositivo. • Decodificar e analisar dados do Google Maps. • Recuperar dados adicionais do Chrome e baseados no navegador para incluir em suas investigações.

Observação: Após a conclusão bem-sucedida do exame de Análise avançada de smartphone da Cellebrite (CASA) e do teste de habilidades práticas, você receberá uma credencial de certificação em Análise avançada de smartphone da Cellebrite.

Seja qualificado. Seja certificado.

Todos os dias, os dados digitais estão afetando as investigações no mundo todo. Torná-los inteligentes e úteis é a especialidade da Cellebrite. A Academia da Cellebrite reflete nosso compromisso com a excelência em perícia digital, treinando examinadores forenses, analistas, investigadores e promotores em todo o mundo para atingir o padrão mais alto de competência e sucesso profissional.

Saiba mais no site cellebritelearningcenter.com

Cellebrite Digital intelligence for a safer world

Rev. CASA 10-18 (PT)