Operador certificado pela Cellebrite (CCO)

Treinamento forense global

Nível
Intermediário

Duração
Dois dias (14 horas)

Público-alvo
Analistas, investigadores e peritos móveis principais

Modo de apresentação
Treinamento conduzido por instrutor, Online On-Demand

Descrição do curso

O curso de Operador certificado pela Cellebrite (CCO), com duração de dois dias, é um valioso programa de certificação forense móvel, com ênfase extraordinária no operador de ferramentas de perícia digital.

Imediatamente após as apresentações básicas, sem perda de tempo, os participantes começam atividades práticas instalando software e fazendo a pré-extração de dispositivos. O programa de CCO foi projetado para melhorar os fluxos de trabalho de perícia digital, expondo os participantes a uma arquitetura linear de coleta, exame e pós-processamento de provas.

O curso foi projetado para acomodar os estilos passivos e ativos de alunos. Cada módulo e tópico inclui dinâmicas para incentivar a recepção, o processamento e a retenção das habilidades necessárias para operar o Touch 2, o 4PC e o Physical Analyzer para clonagem de cartões SIM, conclusão de extrações com bootloaders e outras técnicas, solução de problemas em extrações problemáticas de dispositivos móveis e dispositivos de triagem a fim de criar relatórios para acelerar o atendimento de casos.

Além do uso dos produtos da Cellebrite para concluir os muitos exercícios práticos no curso de CCO, este se concentra nas habilidades, nas qualificações e nos conhecimentos observáveis e mensuráveis que são adequadas a um curso de certificação legítimo, que atende aos padrões da Quality Matters. A Cellebrite acredita na responsabilidade de ensinar aos membros da comunidade de perícia digital as competências necessárias para realizar exames de forma ética, usando normas profissionais universais.

Objetivos do curso

Após a conclusão bem-sucedida deste curso, o aluno será capaz de:

- Instalar e configurar o Touch, Touch2 ou 4PC e o software UFED Physical Analyzer.
- Explicar as melhores práticas para identificação na cena, coleta, embalagem, transporte, exame e armazenamento de dados e dispositivos com provas digitais.
- Exibir as melhores práticas ao realizar extrações de celulares.
- Identificar funções usadas com Touch, Touch2 ou 4PC para realizar as extrações de dados suportadas.
- Usar a geração de relatórios de triagem para investigação.
- Demonstrar proficiência nos objetivos de aprendizado acima sendo aprovado em um teste de conhecimento e avaliação de habilidades práticas com pontuação igual ou superior a 80%.

Módulo	Descrição e objetivos
Introdução	• Descrição do processo principal de treinamento e certificação da Cellebrite • Explanação sobre os prêmios e as realizações da Cellebrite • Reconhecimento dos recursos das soluções de perícia digital e plataformas da Cellebrite • Explicação das responsabilidades legais dos profissionais ao usar produtos, softwares e serviços da Cellebrite
Manuseio forense de dispositivos móveis	• Reconhecimento das considerações jurídicas relacionadas à apreensão e pesquisa em dispositivos. • Exame das tecnologias de dispositivos móveis e da Internet das Coisas (IoT) que são úteis em uma investigação • Descrição das fases do processo de perícia digital • Descrição dos procedimentos corretos para que agentes de campo identifiquem e manuseiem dispositivos com provas digitais • Identificação de dispositivos na cena (marca e modelo) • Identificação de vários mecanismos de bloqueio encontrados em dispositivos móveis • Explicação das melhores práticas para documentar as investigações de dispositivos móveis • Técnicas de pesquisa no Reader • Técnicas e considerações de blindagem e isolamento • Descoberta dos procedimentos de coleta de dispositivos no estado ligado • Descoberta dos procedimentos de coleta de dispositivos no estado desligado
Familiarização com Touch2 e 4PC	• Lista de componentes, recursos ou funções do Touch2 e 4PC • Descrição de como comprar e manter a licença da tecnologia UFED • Discussão sobre como atualizar software e firmware no Touch2 e 4PC • Implementação e instalação de 4PC em uma estação de trabalho de computador • Modificação das configurações de Touch2 e 4PC para a extração de diferentes dispositivos e diferentes necessidades de investigação
Metodologia de extração da Cellebrite	• Melhores práticas para extrações • Bloqueios de tela no Android • Senhas em dispositivos iOS • Tipos de cartão SD • Explicação da organização do sistema de arquivos do SIM • Extrações e clonagens de cartão SIM usando Touch2/4PC • Uso do cabo de alimentação do celular • Extrações de UFED • Abordagens de extração de dados • Opções de métodos de extração • Interfaces de conexão de extração • UFED Camera Services

Módulo	Descrição e objetivos
Metodologia de extração da Cellebrite	• Métodos de extração explicados – Físicos • Métodos de extração explicados – Físicos com cliente • O que é bootloader? • Extrações de sistema de arquivos explicadas • Métodos de extração explicados – Sistema de arquivos • Extrações com o Physical Analyzer • Saída de extrações lógicas avançadas para iOS descrita • Técnicas de rolagem manual • Manuseio de provas pós-extração • Perguntas frequentes sobre métodos de extração (lógica, sistema de arquivos, backup do Android, downgrade de APK, extração física, ADB avançado, ADB avançado (genérico), ABD (rooting), bootloader, ADB inteligente, CAS, EDL, bloquear/ignorar senha)
Geração de relatórios de triagem	• Geração de relatórios de triagem – Dados de usuário • Relatórios de triagem para investigação adicional • Obstáculos à análise de triagem • Triagem e Reader como multiplicadores de forças • Recursos do Reader • Triagem com Physical Analyzer • Triagem de SMS que pode exigir decodificação adicional • Pesquisas e filtros - Visão geral • Marcação de itens de interesse • Início da criação de um relatório de triagem • Assistente de relatório • Geração de relatório • Senhas e criptografia • Software do Reader • Geração de relatórios - O que fazer depois que o Reader é distribuído

Aviso importante: os materiais necessários para o CCO estão disponíveis online sob demanda.

A aulas Online On-Demand foram projetadas para alunos que já possuem ou têm acesso a hardware e software da Cellebrite, com licença atualizada, antes do início das aulas. Os alunos que ainda não possuem ou têm acesso a hardware e software da Cellebrite com licença atualizada são incentivados a participar de nossas aulas conduzidas por instrutor ou online em tempo real.

Leia mais sobre Hardware, software e materiais necessários para nossas aulas Online On-Demand em: cellebritelearningcenter.com

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. CCO 12-18 (PT)