

# Analista físico certificado pela Cellebrite (CCPA)

Treinamento forense global



## Nível

Avançado

## Duração

Três dias (21 horas)

## Público-alvo

Equipes de perícia,  
investigadores

## Modo de apresentação

Treinamento conduzido  
por instrutor, Online  
On-Demand

## Descrição do curso

O curso de Analista físico certificado pela Cellebrite (CCPA) é um programa de nível avançado, com duração de três dias, projetado para investigadores com conhecimento técnico, analistas de provas digitais e profissionais forenses. Como este curso é voltado para análise e técnicas avançadas de pesquisa usando o UFED Physical Analyzer, os participantes NÃO farão extrações de dispositivos durante ele. O software UFED Physical Analyzer será usado extensivamente para explorar dados excluídos recuperados, conteúdo de bases de dados, técnicas avançadas de pesquisa e análise, verificação, validação e geração de relatórios.

Os alunos receberão a certificação de CCPA se forem aprovados em um teste de conhecimento e avaliação de habilidades práticas com pontuação igual ou superior a 80%. A única maneira de obter a certificação de CCPA é fazendo o exame juntamente com um curso associado; não está disponível um teste para isentá-los desse curso.

Antes de fazer este curso, é altamente recomendável que os alunos concluam o curso de Fundamentos de perícia móvel da Cellebrite (CMFF), ou o respectivo teste para isentá-los desse curso, bem como o curso de Operador certificado pela Cellebrite (CCO).

## Objetivos do curso

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

- Realizar análises forenses avançadas em dispositivos móveis.
- Lembrar de técnicas usadas para autenticação e validação.
- Identificar funções no software Physical Analyzer que permitem o exame de vários tipos de dados.
- Gerar relatórios personalizados.
- Demonstrar proficiência sendo aprovado em um exame.

Módulo	Descrição e objetivos
<b>Introdução</b>	<ul style="list-style-type: none"><li>• Introdução e administração do curso</li><li>• Materiais do curso</li><li>• Apresentação dos instrutores</li><li>• Apresentação dos participantes</li><li>• Visão geral da Cellebrite</li></ul>
<b>Visão geral do UFED Physical Analyzer</b>	<ul style="list-style-type: none"><li>• Instalação e licenciamento</li><li>• Configuração</li><li>• Configuração de arquivos de dados</li><li>• Recursos de geração de relatórios</li><li>• Formatos de relatórios</li><li>• Personalização de relatórios</li><li>• Recursos</li><li>• Abertura de extração física</li><li>• Painel de informações de dispositivo</li><li>• Verificação de hashes de imagem</li><li>• Análise de provas digitais adquiridas</li><li>• Dados analisados</li><li>• Espaço de trabalho</li><li>• Análise de linha de tempo</li><li>• Gerenciador de definição de hash</li><li>• Verificação de malware</li></ul>
<b>Introdução à análise de smartphone</b>	<ul style="list-style-type: none"><li>• Principais problemas de investigação do Android</li><li>• Atributos de sistema de arquivos do Android</li><li>• Definição de rooting</li><li>• Noções básicas de sistema de arquivos do Android</li><li>• Visão geral do iOS</li><li>• Principais problemas de investigação do iOS</li><li>• Definição de jailbreaking</li><li>• APFS (sistema de arquivos Apple)</li><li>• Exemplo de contêiner APFS</li><li>• HFS, HFS+ e HSFx (Sistema de Arquivo Hierárquico)</li><li>• Comparação de APFS/HFS+/EXT4</li><li>• Similaridades do Android com iOS</li></ul>

Módulo	Descrição e objetivos
<p><b>Técnicas de análise de dados</b></p>	<ul style="list-style-type: none"> <li>• Physical Analyzer - Opção avançada de abertura</li> <li>• Physical Analyzer – Cadeia de plugins</li> <li>• Physical Analyzer – Gerenciador de cadeia</li> <li>• Physical Analyzer - Alocação de dados de imagem</li> <li>• Physical Analyzer - Alocação de dados automatizada</li> <li>• NAND ou NOR</li> <li>• Physical Analyzer - Organização de flash NAND</li> <li>• Coleta de lixo</li> <li>• Setor defeituoso</li> <li>• Camada de conversão de flash NAND</li> <li>• Physical Analyzer - Exemplo de gravação e exclusão</li> <li>• Esquemas de codificação de dados</li> <li>• Binário, bytes e WORDs simplificados</li> <li>• O que é o sistema de valor decimal?</li> <li>• Hexadecimal</li> <li>• O que é o sistema de valor hexadecimal?</li> <li>• Formatos Big-Endian e Little-Endian</li> <li>• Tabelas de codificação ACSII</li> <li>• Amostra de SMS de 7 bits</li> <li>• PDU de 7 bits de SMS</li> <li>• Informações invertidas (alternadas) de nibble</li> <li>• Physical Analyzer - Pesquisa avançada - Localizar</li> <li>• Physical Analyzer - Guia de valores</li> <li>• Physical Analyzer - Dados hexadecimais de destaques</li> <li>• Physical Analyzer - Quadro de informações</li> </ul>
<p><b>Familiarização com o SQLite Wizard</b></p>	<ul style="list-style-type: none"> <li>• Visão geral de bases de dados SQLite</li> <li>• Estruturas de bases de dados SQLite</li> <li>• Visualização de dados SQLite</li> <li>• Junções de tabela</li> <li>• SQLite Wizard</li> </ul>
<p><b>Verificação e validação</b></p>	<ul style="list-style-type: none"> <li>• Métodos de verificação e validação</li> <li>• Técnicas de rolagem manual</li> <li>• Ferramentas de terceiros</li> <li>• Uso de bases de dados SQLite para validação</li> </ul>
<p><b>Geração de relatórios</b></p>	<ul style="list-style-type: none"> <li>• Elementos do relatório</li> <li>• Elementos do relatório - Estabelecimento de credibilidade</li> <li>• Dados do relatório - Inclusão ou exclusão</li> <li>• Elementos do relatório - Aquisição de provas digitais</li> <li>• Elementos do relatório - Análise de provas digitais</li> <li>• Localização e diretório de relatório</li> <li>• Recursos de geração de relatórios do Physical Analyzer</li> <li>• Formatos de relatório do Physical Analyzer</li> <li>• Personalização de relatórios do Physical Analyzer</li> <li>• Physical Analyzer - Campos adicionais</li> <li>• Elementos do relatório do Physical Analyzer - Resumo</li> </ul>
<p><b>Exame final/prático</b></p>	<p>É oferecido aos participantes um exame escrito opcional e um teste de habilidades práticas na conclusão do curso. A conclusão bem-sucedida do curso sem tentar ou ser aprovado no exame opcional e no teste de habilidades resulta em um Certificado de conclusão de Analista físico da Cellebrite.</p>

Analista físico certificado pela Cellebrite (CCPA)

**Aviso importante:** os materiais necessários para o CCPA 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](https://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](http://cellebritelearningcenter.com)

Os materiais e tópicos tratados aqui são fornecidos "no estado em que se encontram" e "conforme disponíveis", sem garantias de qualquer tipo, incluindo, por exemplo, garantias de comercialização, adequação a um fim específico ou quanto à sua precisão ou integralidade. Observe que alguns materiais, tópicos e itens aqui fornecidos estão sujeitos a alterações. A Cellebrite não oferece garantias, expressas ou implícitas, para marcas registradas da Cellebrite nos Estados Unidos e/ou em outros países. Outras marcas mencionadas são propriedade de seus respectivos proprietários. A lei aplicável talvez não permita a exclusão de garantias implícitas, de modo que a exclusão acima pode não se aplicar a você.