Vulnerabilidades nos arquivos UFDR da Cellebrite: impactos e riscos da cadeia de custódia

18/07/2025

Este artigo descreve o contexto de uso do software *Cellebrite* no contexto da aquisição de prova digital, estabelecendo previamente a tendência atual das investigações criminais em dados e metadados. Para tanto, situa as definições básicas à compreensão do contextual digital, apontando, ao final, as vulnerabilidades dos arquivos UFDR da *Cellebrite*, com o fim de fornecer elementos à melhoria constante de conformidade probatória no ambiente processual penal.

Do celular ao smartphones: uso e riscos

A passagem da telefonia fixa, para celulares (entre 1973-1993) e smartphones (1994 até hoje) ocorreu de modo incremental, com alterações significativas quanto à estrutura, riscos e funcionalidades.

Celular é o dispositivo de comunicação móvel que permite fazer e receber chamadas telefônicas sem fio, utilizando ondas de rádio através de uma rede de torres de transmissão (antenas celulares). Hoje coisa quase de museu.

Smartphone (telefone inteligente) é um tipo avançado de celular que combina as funções tradicionais de um telefone móvel com recursos de um computador portátil (celular com capacidades computacionais expandidas). Atualmente dobráveis, integrados a modelos de Inteligência Artificial, dentre outras funcionalidades, os smartphones armazenam e produzem dados e metadados.

Segundo a pesquisa realizada pela FGV, em 2024, o Brasil tinha em uso 480 milhões de dispositivos digitais (computador, notebook, tablet e smartphone), sendo que ***cada habitante usava 1,2 smartphones, totalizando 258 milhões de dispositivos***. Você conhece poucas pessoas sem smartphones (conta nos dedos). E o seu smartphone produz e armazena dados e metadados. **Eis o ponto relevante**.

Dados

Dados digitais são os registros primários do conteúdo principal armazenado em formato eletrônico, representado pelo que o usuário visualiza ou manipula diretamente, como: a) Dados textuais (e-mails; mensagens instantâneas — Whatsapp etc.; documentos; código-fonte etc.); b) Dados multimídia (imagens jpg, png, gif, svg etc.; áudios mp3, wav etc.; vídeos mp4, avi, mov etc.; dentre outros); c) Dados estruturados (banco de dados; planilhas, arquivos JSON, XML etc.); e, d) Dados de sistema (configurações; memória cache; cookies etc.)

Copyright © 2026 Consultor Jurídico

Metadados

Metadados são "*dados sobre dados*" : informações que descrevem, contextualizam e fornecem detalhes técnicos sobre os dados principais, incluindo a criação, modificação, localização e características técnicas, classificados em: a) Metadados descritivos (título, assunto, autor; descrição do conteúdo; classificação etc.); b) Metadados técnicos (formato, tamanho, resolução, codec, versão etc.); c) Metadados temporais (data e hora da criação, modificação, último acesso; histórico de versões etc.); d) Metadados de localização (GPS, Exif, IP, localização geográfica, fuso horário etc.); e) Metadados de sistema (sistema operacional, aplicativo, versão, dispositivo de criação etc.); e, f) Metadados forenses (hash, assinatura digital etc.).

Exemplo de metadados de uma fotografia: a) Data/hora: 15/07/2025 14:30:25; b) Localização GPS: -23.5605, -46.6333 (São Paulo); c) Câmera: iPhone 14 Pro; d) Resolução: 4032×3024 pixels; e, d) Tamanho: 2.5 MB.

Em termos metafóricos, o *smartphone* funciona como um baú de dados: à primeira vista opaco, mas que, uma vez aberto por técnicas forenses, revela um tesouro informacional escondido (latente). Cada aplicativo opera como um repositório secreto, sendo que os metadados representam as pegadas invisíveis no solo digital, guiando o investigador na reconstrução de vínculos e eventos. Assim como um arqueólogo digital, o perito descobre vestígios enterrados em camadas sucessivas de dados, sendo que em cada clique, mensagem ou foto armazenada funciona como uma chave que abre compartimentos ocultos do contexto investigado.

Prova digital

Prova digital é qualquer informação armazenada ou transmitida em formato digital que pode ser utilizada como evidência em investigações criminais e processos judiciais, incluindo tanto os dados quanto os metadados. Para validade, deve observar a cadeia de custódia.

Cadeia de custódia da prova digital

A cadeia de custódia da prova digital é o processo de documentação ininterrupto da coleta, preservação, análise e apresentação de evidências digitais, garantindo sua integridade, autenticidade, confiabilidade e rastreabilidade desde a origem até sua utilização em procedimentos legais. Garante a validade da prova digital, evitando a contaminação, alteração ou manipulação indevida. Enquanto os dados fornecem o conteúdo, os metadados atestam a conformidade do processo.

Tendência internacional de investigação em metadados e prova digital

A tendência mundial nas investigações criminais deslocou o eixo tradicional da prova física para o domínio das provas digitais, com destaque para os metadados. Órgãos como FBI, *Scotland Yard*, Nist e Interpol padronizam protocolos para coleta, preservação e análise de evidência digital (Berkley, Convenção de Budapeste; ABNT etc.), reconhecendo que os metadados (dados sobre dados: registros técnicos como data, hora, localização e autoria) constituem elementos probatórios relevantes à formulação da hipótese criminal sobre o caso penal.

Copyright © 2026 Consultor Jurídico

A validade da prova depende da integridade da cadeia de custódia dos registros, que devem estar integrados a mecanismos verificáveis [logs de acesso; códigos hash etc.). A tendência é a prevalência das fontes digitais no ambiente da investigação criminal, como demostram as investigações criminais que raramente não buscam a apreensão de um smartphone e seu "tesouro escondido".

Extração de dados

A extração de dados de smartphones ocupa papel central nesse processo. Ferramentas como Cellebrite, GrayKey, Magnet Axiom, Ávila Forense e Oxygen Forensic viabilizam a extração lógica, física ou avançada de dados armazenados ou apagados. A maioria dos dispositivos contém dados sensíveis que vão além do conteúdo visível ao usuário: registros de chamadas, conversas, geolocalizações, arquivos temporários e até fragmentos de memória que revelam comportamentos, vínculos sociais, financeiros e trajetórias geofísicas. A prova digital é adquirida diretamente dos hábitos digitais do usuário, disponíveis por meio de softwares especializados.

Nesse cenário, a empresa Cellebrite tornou-se uma das maiores referências mundiais, fornecendo equipamentos e programas especializados em extrair e analisar dados de dispositivos móveis, mesmo quando estão bloqueados, protegidos por senhas ou criptografados.

O que é Cellebrite?

É uma empresa israelense que desenvolve ferramentas de extração, análise e decodificação de dados digitais adquiridos de dispositivos móveis (smartphones, tablets), tendo como produto principal o Ufed (*Universal Forensic Extraction Device*), permitindo acessar, copiar e organizar dados armazenados em dispositivos eletrônicos, inclusive os apagados, protegidos por senha ou criptografados.

Para que serve?

Serve para fins periciais e de investigação criminal, possibilitando que órgãos de segurança, perícia e Ministério Público obtenham provas digitais de forma automatizada, a partir da geração de arquivos como o UFDR (*Universal Forensic Digital Report*), que contém os dados extraídos organizados em formato de relatório.

Como funciona?

Funciona conectando o dispositivo (smartphone; tablet etc.) ao sistema Cellebrite, que utiliza métodos de extração lógica, física ou avançada (via exploits), a depender do modelo e do sistema operacional. Após a extração, os dados são processados, indexados e exportados em formatos legíveis para análise e eventual caso penal.

Ferramentas como o ***Cellebrite Ufed*** (*Universal Forensic Extraction Device*) são amplamente utilizadas por órgãos públicos, polícias, Ministério Público, advogados, peritos e empresas de segurança digital, permitindo acessar, copiar e registrar dados de celulares, como mensagens, fotos, conversas de aplicativos, registros de chamadas e muito mais. Para apresentar esses

Copyright © 2026 Consultor Jurídico

dados de forma organizada, o sistema gera relatórios em arquivos chamados **.UFDR**, que podem ser lidos até por quem não possui o programa completo da Cellebrite, usando apenas o ***Cellebrite Reader***.

No entanto, mesmo sendo muito confiáveis e reconhecidas no mercado, essas ferramentas, como qualquer software, podem ter vulnerabilidades/falhas que colocam em risco a integridade das provas digitais. Vamos especificar melhor.

UFD e UFDR: qual a diferença?

Vamos estabelecer a diferença entre os dois tipos de arquivos da Cellebrite que frequentemente geram confusão: o *UFD* e o *UFDR*. Apesar de parecidos nos nomes, eles têm funções bem diferentes.

[a] UFD: o arquivo *UFD* é criado no momento da *extração dos dados* do celular, armazenando as informações técnicas sobre essa coleta, como data, horário, tipo de cabo usado e versão do equipamento. Mais importante: contém uma assinatura digital especial (*HMAC*), que serve como uma espécie de "cadeado" para garantir que nada ali foi alterado depois. Se alguém tentar mexer nesse arquivo, o sistema consegue identificar que ele foi modificado.

[b] UFDR: o arquivo *UFDR* é criado depois, durante o processamento dos dados que foram extraídos, produzindo uma espécie de "relatório", gerado pelo programa *Cellebrite Physical Analyzer*, com o fim de organizar os dados para consulta (mensagens, fotos, contatos etc.), favorecendo a visualização e análise operacional do conteúdo por peritos, investigadores, advogados e autoridades, inclusive por meio do *Cellebrite Reader*.

Em resumo: Enquanto o *UFD* é um registro técnico da coleta bruta dos dados, o *UFDR* é o documento que permite visualizar de modo estruturado e acessível, o conteúdo coletado.

Sobre a vulnerabilidade

É inegável que o Cellebrite UFED é uma ferramenta fundamental na perícia digital. Porém, como qualquer programa de computador, também pode apresentar vulnerabilidades que precisam ser conhecidas pelos operadores do Direito.

Pesquisas recentes conduzidas por Daniel Avilla revelaram que é possível alterar ou manipular os dados contidos nos arquivos .UFDR. Na prática, alguém que tenha acesso apenas ao arquivo UFDR poderia modificá-lo, por exemplo, para alterar mensagens de WhatsApp, incluir ou apagar registros e, depois, reconstruir o arquivo. Isso ocorre porque o UFDR nada mais é do que um arquivo "compactado", que pode ser aberto como uma pasta (por exemplo, renomeando sua extensão para .zip) e editado. Dentro dele, há arquivos em texto simples (p.ex. *report.xml*) que contêm dados como conversas ou listas de arquivos encontrados.

Depois de fazer as alterações, basta compactar tudo novamente e renomear o arquivo para UFDR e abri-lo no *Cellebrite Reader*. Embora o programa possua um mecanismo de verificação que pode gerar um alerta de integridade, detectando a modificação do arquivo original, existe um problema: o Cellebrite Reader permite gerar um novo arquivo UFDR a partir desse arquivo

Copyright © 2026 Consultor Jurídico

adulterado. Quando isso acontece, esse novo UFDR pode aparentar estar completamente íntegro, escondendo a manipulação indevida, porque é reconhecido como válido pelo sistema e não retorna mais nenhum erro de integridade. Após isso, o UFDR original pode ser excluído e apenas o modificado armazenado ou compartilhado.

Essa vulnerabilidade representa um risco muito sério para a cadeia de custódia e para a segurança jurídica das provas digitais. Ainda mais porque, em muitos laboratórios forenses, existe o costume de não preservar o arquivo *UFD* por muito tempo, seja por questão de espaço físico ou custo. Muitas vezes, apenas o *UFDR* é mantido e enviado junto às mídias que vão para o Ministério Público ou para o Judiciário.

Se o arquivo *UFD* estiver indisponível e o dispositivo original (smartfone) também não puder ser novamente periciado, a existência apenas do arquivo UFDR ***não garante plenamente a integridade das provas apresentadas*** porque sujeito à manipulação indevida anteriormente descrita, a seguir visualizada.

Demonstração prática: prova de conceito

Figura 1 – Tela do *Cellebrite Reader*. À esquerda, o relatório UFDR original; à direita, o relatório UFDR modificado.

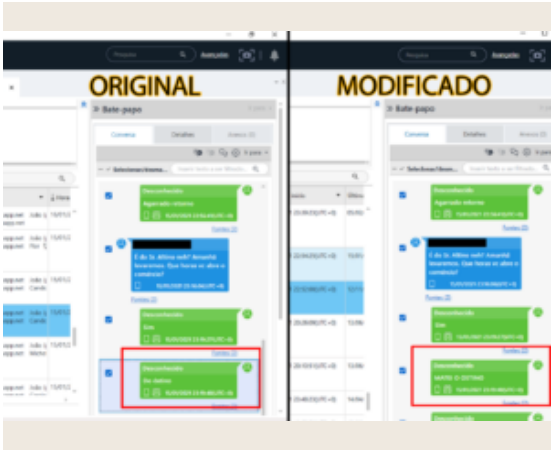
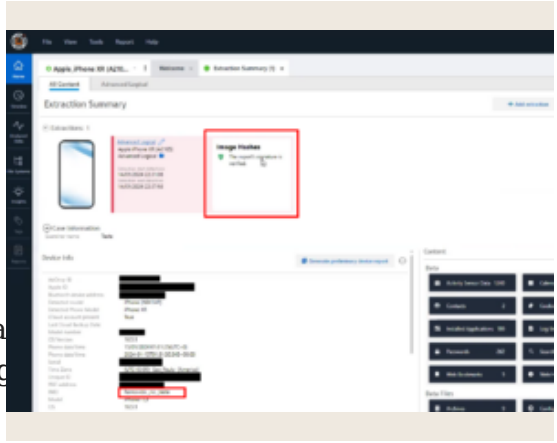


Figura 2 – Tela do Cellebrite Reader. Exemplo de assinatura válida em um arquivo UFDR modificado. Na aba Imei por exemplo removi o conteúdo.



Conclusão

Smartphones tendem a ser cada vez mais fontes de provas, exigindo-se a custódia da prova dig softwares.

No caso da Cellebrite, a possibilidade de adulterar arquivos ***.UFDR*** mostra que não basta confiar apenas nos relatórios gerados para a análise das provas digitais. É fundamental manter o arquivo ***.UFD*** armazenado, assegurando meios de contraprova, porque possui mecanismos muito mais robustos de integridade, servindo como elemento de verificação caso haja alguma dúvida sobre a autenticidade, confiabilidade ou rastreabilidade dos dados e metadados.

Profissionais do Direito precisam estar cientes dos limites e possibilidades das ferramentas, evitando nulidades ou questionamentos judiciais sobre provas digitais que, à primeira vista, parecem confiáveis. É essencial exigir sempre que, junto ao UFDR, sejam preservados os

Copyright © 2026 Consultor Jurídico

arquivos originais e a documentação técnica completa, garantindo-se o devido processo legal digital.

Num mundo em que a tecnologia evolui rapidamente, mostra-se indispensável que o Direito acompanhe essa evolução, compreendendo as possibilidades, limites e os riscos associados à produção de provas digitais.

P.S. Se você "flopou" ao não entender o tema abordado, é sinal de que há um mundo digital a ser descoberto, porque a prova digital não é um hype (passageiro). Ela veio para ficar. Comparece cada vez mais nas investigações criminais. Reconhecer lacunas de aprendizagem é um sinal de força, porque ativa a disposição para reaprender as coordenadas de um novo mundo, diferente do analógico que estávamos acostumados. Conte conosco.

Fonte: https://conjur.jumps.com.br/2025-jul-18/vulnerabilidades-nos-arquivos-ufdr-da-cellebrite-impactos-e-riscos-da-cadeia-de-custodia/

Copyright © 2026 Consultor Jurídico