T. F. Baldasso, G. M. Alvarez, Rev. Bras. Crim. 2026
Edição Especial dos Anais do XXVIII Congresso Nacional de Criminalística

2026
ISSN 2237-9223

REVISTA BRASILEIRA DE CRIMINALÍSTICA

Edição Especial dos Anais do

Formatos Digitais de Arquivos de Imagem na Fotografia Criminalística: Integridade e Valor Probatório

T. F. Baldasso[a,*], G. M. Alvarez[a]

[a]*Instituto-Geral de Perícias, Secretaria da Segurança Pública do Estado do Rio Grande do Sul, Porto Alegre (RS), Brasil*
[*]*Endereço de e-mail para correspondência: tiago-baldasso@igp.rs.gov.br. Tel.: +55-51-98285-9825.*

Palavras-chave: fotografia criminalística; RAW; cadeia de custódia; hash; prova digital.

1. INTRODUÇÃO

A motivação principal deste trabalho centra-se na necessidade de discutir como a fotografia digital vem sendo produzida, tratada e preservada na rotina pericial, especialmente nos registros fotográficos de local de crime. A fotografia criminalística registra mais do que uma imagem da cena: documenta vestígios, posições, condições de iluminação e outros elementos que podem influenciar a interpretação do fato investigado. Com o meio digital, esse registro tornou-se mais rápido, mas passou a depender de escolhas técnicas relacionadas ao formato do arquivo, compressão, metadados, processamento e arquivamento. Esses aspectos interferem diretamente na integridade, na rastreabilidade e no valor probatório da imagem.

Para tanto, o trabalho se apoia em referências da fotografia forense, da prova digital e de protocolos institucionais. Robinson, Duncan, Marsh, Staggs e Toledo tratam de captura, processamento, RAW, EXIF, cadeia de custódia e preservação do original [1-5]. Marques, Paciarelli e o Manual de Cadeia de Custódia do Espírito Santo reforçam a discussão sobre hash, metadados, autenticidade e integridade [6-8]. Também foram considerados documentos do SWGDE, SWGIT, Santa Barbara County Sheriff's Office e Oregon State Police, nos quais se observa que o formato do arquivo deve acompanhar a finalidade pericial do registro [9-12].

De uma forma prática, observa-se que muitas fotografias são convertidas, compartilhadas e arquivadas sem preservação clara do arquivo original. O JPEG é amplamente utilizado por sua praticidade e compatibilidade, porém corresponde a uma imagem já processada, comprimida e com perda de informação. Quando esse arquivo passa a ser a única versão armazenada, tornam-se mais limitadas a verificação de edição, a recuperação de dados da captura e a realização de contraprova técnica consistente. O RAW, por sua vez, preserva mais dados do sensor e funciona melhor como matriz da captura.

Há de se ressaltar que essa discussão ganha força diante da facilidade atual de edição digital, inteligência artificial e geração sintética de imagens. Nesse contexto, a diferença entre guardar apenas uma imagem finalizada e preservar a matriz original deixa de ser detalhe técnico e passa a ter efeito probatório [13]. Assim, o objetivo deste trabalho é discutir a relevância dos formatos digitais na fotografia criminalística, com foco na preservação do original, metadados, hash e rastreabilidade do fluxo pericial.

2. METODOLOGIA

O estudo é bibliográfico, descritivo e experimental. A parte bibliográfica reuniu obras de fotografia forense, prova digital, cadeia de custódia, formatos de imagem e protocolos institucionais. A parte experimental comparou arquivos derivados de uma mesma captura, observando compressão, metadados, processamento posterior e integridade digital.

Foi utilizado registro fotográfico obtido em levantamento fotopericial com uso de luminol, cuja reação quimioluminescente exige controle de exposição,

foco e preservação do arquivo original. A captura foi feita com câmera Nikon D5300, lente Nikon AF-P DX Nikkor 18-55 mm, ISO 800, exposição de 15 segundos, distância focal de 18 mm e compensação de exposição de 0 EV.

O arquivo foi produzido em RAW/NEF. A partir dele, foram analisadas versões em JPEG, incluindo imagens editadas no GIMP 3.2.2 com inserção artificial de luminescência alusiva ao luminol e de arma de fogo. Também foram avaliados metadados, arquivo auxiliar .pp3 do RawTherapee 5.0 e hashes SHA-256 gerados no Windows PowerShell pelo comando Get-FileHash.

A comparação considerou quatro arquivos: matriz RAW, JPEG gerado a partir do NEF, derivado com luminescência artificial e derivado com arma de fogo artificial. A intenção não foi testar um software específico, mas mostrar como formato, metadados, processamento e hash ajudam a separar original, cópia de trabalho e imagem editada, especialmente diante da facilidade atual de edição digital e geração sintética de imagens.

3. RESULTADOS E DISCUSSÃO

Os testes indicaram diferenças relevantes entre os arquivos analisados. De uma forma prática, observou-se que o JPEG atende melhor às demandas de compatibilidade com dispositivos e softwares, facilitando a visualização, o compartilhamento e a inserção em laudo. Há de se ressaltar, contudo, que essa praticidade ocorre acompanhada de compressão com perdas. Assim, parte das informações originalmente captadas pode ser descartada, principalmente quando o arquivo passa por edições e salvamentos sucessivos. A Figura 1 apresenta a versão JPEG usada como referência na comparação.



Figura 1. Versão JPEG do registro fotográfico utilizada como referência de comparação no experimento.

O RAW preservou mais dados do sensor fotográfico. Isso ampliou a margem de recuperação tonal e manteve informações técnicas da captura. Ele não impede a criação de cópias editadas, mas preserva a matriz original e permite distinguir o registro inicial das versões depois geradas.



Figura 2. Arquivo RAW/NEF original, preservado como matriz primária da captura.

A primeira versão derivada recebeu inserção artificial de luminescência azulada. A alteração é visualmente compatível com o contexto do luminol, mas sugere um vestígio que não estava registrado na imagem original. Esse tipo de intervenção pode modificar a leitura técnica da cena.



Figura 3. Versão derivada com inserção artificial de luminescência azulada.

A segunda versão derivada recebeu inserção artificial de arma de fogo. A alteração é ainda mais sensível, pois introduz elemento com possível relevância criminalística e pode alterar diretamente a interpretação do ambiente examinado.



Figura 4. Versão derivada com inserção artificial de arma de fogo.

As imagens derivadas deixam claro o problema: uma alteração que parece combinar com o ambiente pode inserir informação que não existia na cena. Por isso, preservar o RAW, os metadados e os registros de processamento ajuda a separar o que é captura original, cópia de trabalho e imagem editada.

O hash serviu para individualizar os arquivos e confirmar que RAW, JPEG e derivados são arquivos diferentes. Ele não diz, sozinho, se a imagem é verdadeira ou falsa, mas ajuda a verificar se o arquivo foi alterado. Os códigos alfanuméricos foram gerados no Windows PowerShell, por meio do comando Get-FileHash. Na tabela, os valores foram abreviados para facilitar a leitura.

Tabela 1. Síntese dos arquivos utilizados na comparação experimental.

Arquivo	**Função no experimento**	**Constatação**	**Hash SHA-256 abreviado**
DSC_1024.NEF	Matriz RAW da captura	Preserva mais dados do sensor e parâmetros técnicos.	3196AE84...795FC9675
DSC_1024-1.jpg	Versão JPEG	Imagem processada e comprimida pela câmera.	8F2CA8D3...1419ACACF
DSC_1024-2.jpg	Derivada com luminescência	Insere vestígio visual inexistente no registro original.	9228D7C2...72154A50
DSC_1024-3.png	Derivada com arma de fogo	Altera a leitura técnica da cena.	C5AD21D6...F4A30530

Os metadados EXIF também entram nesse controle. Eles indicam câmera, lente, data, ISO, tempo de exposição, abertura, distância focal e flash. Não substituem a cadeia de custódia, mas ajudam a conferir se o arquivo combina com o equipamento e com o contexto informado. Como exemplo adicional, a Fig. 5 apresenta a visualização de outro arquivo RAW/NEF no RawTherapee, com exibição dos metadados técnicos da captura.

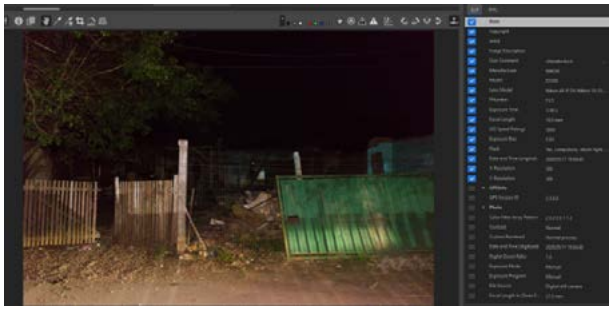


Figura 5. Arquivo RAW/NEF visualizado no RawTherapee, com metadados técnicos da captura.

O arquivo .pp3, gerado pelo RawTherapee, registrou os ajustes de revelação sem modificar o RAW. Isso ajuda a mostrar o que é matriz original e o que é processamento posterior.

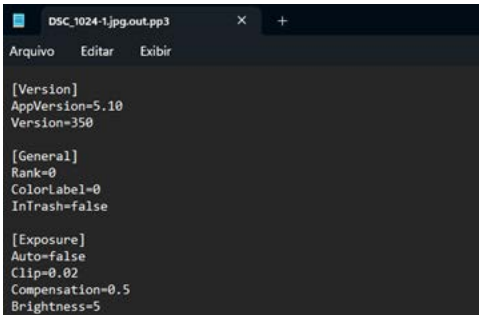


Figura 6. Arquivo .pp3 gerado pelo RawTherapee, registrando parte dos ajustes de revelação sem modificar o RAW original.

No contexto pericial, fotografar não acaba no clique. A confiabilidade da imagem depende de controle técnico sobre captura, preservação, processamento, documentação e rastreabilidade dos arquivos.

4. PROPOSTAS DE PADRONIZAÇÃO

A partir dos pontos discutidos, nota-se que algumas medidas simples podem contribuir para melhorar o manejo da fotografia criminalística digital. A intenção não é propor um fluxo inviável para a rotina pericial, mas estabelecer condições mínimas de controle sobre arquivos que podem assumir valor probatório.

De uma forma prática, a primeira medida diz respeito à padronização dos nomes de pastas e arquivos. Nomes automáticos gerados pela câmera, como DSC_1024 ou IMG_0001, dificultam a organização, a localização posterior e a vinculação das imagens ao procedimento. Para tanto, entende-se como adequado que cada pasta e cada conjunto de imagens estejam relacionados ao número do protocolo, ocorrência ou procedimento pericial.

Também há de se considerar a guarda adequada dos arquivos RAW. Embora ocupem mais espaço que o JPEG, esses arquivos preservam maior quantidade de informações da captura. Isso exige planejamento de armazenamento, rotina de backup, controle de acesso e organização do acervo digital. Toledo [5] apresenta tabela sobre guarda e descarte de fotografias periciais com base em prazos prescricionais. A partir dessa lógica, arquivos RAW, JPEG e demais registros digitais podem ser submetidos a regra clara de guarda e descarte. Cumprido o prazo definido em protocolo, o descarte dos RAW pode ser avaliado como forma de

reduzir o volume de armazenamento, desde que sejam mantidos os JPEG necessários e a anotação de quando, como e por quem o descarte foi realizado.

Outra medida importante refere-se à extração e preservação dos metadados EXIF, à geração de hash individual de cada fotografia e também ao hash da pasta que reúne o conjunto de imagens. O hash individual permite conferir cada arquivo separadamente, enquanto o hash da pasta facilita a indicação do conjunto no laudo e o controle do material arquivado.

Há de se ressaltar, ainda, que o fluxo deve separar arquivo original e cópia de trabalho. O RAW deve permanecer preservado como matriz da captura. JPEG, TIFF, PNG ou outros formatos podem ser utilizados para laudo, visualização, comparação ou apresentação, mas não devem substituir o original. Quando houver revelação digital ou ajustes, arquivos auxiliares, como o .pp3 do RawTherapee, ajudam a registrar o processamento sem alterar o RAW.

Nesse sentido, recomenda-se que cada órgão defina responsabilidade técnica clara pelo gerenciamento das fotografias digitais, seja por rotina própria, núcleo especializado ou equipe capacitada para essa finalidade.

5. CONCLUSÕES

A escolha do formato digital não deve observar apenas a praticidade operacional. Na criminalística, a força probatória da fotografia depende tanto daquilo que a imagem mostra quanto da possibilidade de demonstrar sua origem, autenticidade e integridade.

Com os testes realizados, observou-se que o JPEG atende bem às necessidades de visualização, compartilhamento e inserção em laudo. Contudo, quando passa a ser o único arquivo preservado, apresenta maior fragilidade. Por se tratar de imagem já processada e comprimida, reduz a margem de reanálise e dificulta a verificação técnica em situações de questionamento sobre edição, perda de informação ou alteração posterior.

As versões derivadas utilizadas no experimento reforçam essa preocupação. De uma forma prática, verificou-se que alterações visualmente plausíveis podem inserir elementos inexistentes na cena e modificar a leitura pericial do fato. Assim, imagens editadas ou derivadas podem ser utilizadas para apresentação e visualização, desde que o arquivo original seja preservado e os ajustes realizados estejam devidamente identificados.

Há de se ressaltar que, assim como ocorre com vestígios físicos sujeitos a reexame, a fotografia digital também precisa preservar sua matriz original. Quando resta apenas uma imagem finalizada, sem RAW, metadados, histórico de processamento ou hash, torna-se mais limitada a possibilidade de contraprova técnica consistente.

Nesse sentido, propõe-se como encaminhamento uma rotina mínima: preservação do RAW, extração de metadados, geração de hash, separação entre original e cópia, registro dos ajustes, armazenamento seguro e definição de responsabilidade técnica pelo gerenciamento da imagem pericial digital. A legislação já reconhece a fotografia na documentação pericial, mas ainda não detalha critérios próprios para arquivos digitais. Por isso, o tema merece debate específico, especialmente diante da necessidade de futura padronização nacional.

AGRADECIMENTOS

Os autores agradecem à Associação Brasileira de Criminalística e à Associação dos Peritos Criminais do Rio Grande do Sul pela realização do XXVIII Congresso Nacional de Criminalística e pela oportunidade de apresentar esta discussão sobre preservação e rastreabilidade da fotografia criminalística digital. Agradecem também à Associação dos Fotógrafos Criminalísticos pelo suporte disponibilizado e pelo incentivo ao debate técnico da área.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] E.M. Robinson. Crime Scene Photography, 2nd ed., Academic Press, United States of America (2010).

[2] C.D. Duncan. Advanced Crime Scene Photography, CRC Press, United States of America (2010).

[3] N. Marsh. Forensic Photography: A Practitioner's Guide, Wiley-Blackwell, United Kingdom (2014).

[4] S. Staggs. Crime Scene and Evidence Photography, 2nd ed., Staggs Publishing, United States of America (2014).

[5] A. Toledo. Fotografia Pericial, Millennium Editora, Brasil (2025).

[6] A.F.Q.M. Marques. Fotografia forense: contributo para a qualidade em medicina legal. Dissertação de Mestrado, Faculdade de Medicina, Universidade do Porto (2011).

[7] L.R. Paciarelli. Da prova digital no processo judicial. Dissertação de Mestrado, Pontifícia Universidade Católica de Minas Gerais (2024).

[8] Espírito Santo. Polícia Civil. Superintendência de Polícia Técnico-Científica. Manual de Cadeia de Custódia da Perícia Oficial do Espírito Santo, Polícia Civil do Estado do Espírito Santo, Brasil (2021).

[9] Scientific Working Group on Digital Evidence. Digital Image Compression and File Format Guidelines: 16-M-001-3.0, SWGDE (2024).

[10] Scientific Working Group on Imaging Technology. SWGIT Guidelines for the Forensic Imaging Practitioner, International Association for Identification (2016).

[11] Santa Barbara County Sheriff's Office. Photography and Cameras: SOP CSI-008-12, Forensics Unit, United States of America (2012).

[12] Oregon State Police. Forensic Field Guide, Version 12, Oregon State Police Forensic Services Division, United States of America (2024).

[13] Ferdiansyah; M.R.A. Deazwara; R.R. Billanivo; M. Ardiansyah; Ilham. Forensic analysis of AI-generated image alterations using metadata evaluation, ELA, and noise pattern analysis. J. Inf. Syst. Inform. 7: 4014-4035 (2025).