PoC – Analisando Metadados – PhotoShop

01/09/2025

# Relatório de diferenças de metadados

Este documento apresenta a análise realizada por meio comparação de metadados de imagens utilizando a ferramenta Exiftool - (v13.34), com o objetivo de verificar a partir dos metadados das imagens de documentos se houve alteração e edição por programas terceiros.

O **Exiftool** é um utilitário robusto baseado em Perl, amplamente reconhecido na área de análise forense digital por sua capacidade de extrair, modificar e validar metadados de diversos formatos de arquivos. A ferramenta permite o acesso a campos EXIF, IPTC, XMP, além de informações proprietárias de câmeras e softwares de edição, oferecendo uma visão aprofundada sobre a cadeia de manipulação do arquivo. Sua adoção neste relatório se justifica pela confiabilidade dos resultados, suporte a grande variedade de formatos de imagem e precisão na identificação de modificações nos metadados. Além disso, o Exiftool possibilita a automatização de processos via scripts, fator essencial em análises comparativas de grandes volumes de arquivos, garantindo rastreabilidade e integridade na verificação de possíveis alterações introduzidas por programas de terceiros

# Nome da pessoa analisada: Adriana

Identificada pelos **CPF: e RG: Não informado**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a presença de perfis de cor inexistentes no arquivo original e indícios técnicos de reprocessamento (como mudanças no processo de codificação e subamostragem de cor). Esses elementos reforçam a hipótese de edição posterior.**

Pontos importantes:

* FileSize: original 142 kB → alterado 220 kB (aumento)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Thumbnail: 5176 bytes (original) → 5600 bytes (alterado, recriada)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

A análise comparativa demonstra padrão típico de reprocessamento em software de edição (Photoshop/similares), com **Progressive + 4:4:4 + ICC HP** — combinação característica e não compatível com fluxo original de captura. As diferenças no tamanho do arquivo e na miniatura reforçam o indício de manipulação.

**Resultado:** Provável Fraude — 13 pontos (nível **Muito Forte**).

Os metadados e a comparação visual indicam reprocessamento por software de terceiros e inclusão de informação não presente no original.

**Score de indícios:**

* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tamanho do Arquivo (variação relevante) → 1**
* **Miniatura (alterada/recriada) → 1**

**subtotal (score bruto):** **11**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 (Progressive + 4:4:4 em conjunto)**

**Score final (bruto + ajuste): 13 — nível: Muito Forte**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**  
A comparação visual deve ser utilizada como apoio, visto que a versão alterada apresenta diferenças técnicas compatíveis com reprocessamento em editor desktop, reforçando a conclusão de manipulação.

# Nome da pessoa analisada: Cristiano

Identificada pelos **CPF: 015.988.250-89 e RG: não informado**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a presença de perfis de cor Hewlett-Packard inexistentes no arquivo original, além da modificação do processo de codificação e da subamostragem de cor. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 198 kB → alterado 300 kB (aumento compatível com reexportação)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Tags Adobe: presentes no alterado (APP14Flags, ColorTransform)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

A combinação **Progressive + 4:4:4 + ICC HP + Tags Adobe** é assinatura técnica típica de reprocessamento em Photoshop/similares, não compatível com fluxo direto de captura. As alterações de tamanho de arquivo reforçam a conclusão de manipulação digital.

**Resultado: Provável Fraude** — **17 pontos** (nível **Muito Forte**).  
Os metadados indicam reprocessamento por software de terceiros, com inserção de perfis/etiquetas típicas de exportação incompatíveis com uma captura direta de câmera.

**Score de indícios:**

* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tags Adobe/Photoshop → 3**
* **Tamanho do Arquivo (variação relevante) → 1**

**subtotal (score bruto):** **13**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 (Progressive + 4:4:4 em conjunto)**
* **+2 (ICC HP + Adobe/APP14 em conjunto)**

**Score final (bruto + ajuste): 17 — nível: Muito Forte**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A comparação visual pode ser utilizada como apoio, mas os indícios técnicos presentes nos metadados já são suficientes para caracterizar reprocessamento em software de edição desktop.

# Nome da pessoa analisada: Daniel

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a inserção de perfil ICC Hewlett-Packard inexistente no original, bem como a mudança do processo de codificação e da subamostragem de cor. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 129 kB → alterado 194 kB (aumento compatível com reexportação)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Thumbnail: 4546 bytes (original) → 4750 bytes (alterado, recriada)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O conjunto **Progressive + 4:4:4 + ICC HP** caracteriza fortemente reprocessamento em Photoshop/similares. A alteração da miniatura e o aumento do tamanho do arquivo reforçam os indícios de manipulação digital.

**Resultado: Provável Fraude** — **15 pontos** (nível **Muito Forte**).  
Os metadados indicam reprocessamento por software de terceiros, com inclusão de perfil ICC genérico (HP) e mudança técnica consistente (Progressive + 4:4:4).

**Score de indícios:**

* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tamanho do Arquivo (variação relevante) → 1**
* **Miniatura (alterada/recriada) → 1**

**subtotal (score bruto): 11**

**Ajuste qualitativo (Bônus de co-ocorrência)**

* **+2 Progressive + 4:4:4 em conjunto**
* **+2 ICC HP presente em conjunto com Progressive**

**Score final (bruto + ajuste): 15 — nível: Muito Forte**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A comparação visual pode reforçar a conclusão, mas os metadados por si só já demonstram reprocessamento incompatível com uma captura legítima.

# Nome da pessoa analisada: Djailson

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a modificação da orientação, a substituição do processo de codificação e da subamostragem de cor, bem como a inserção de perfil ICC Hewlett-Packard inexistente no original. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 90 kB → alterado 138 kB (aumento compatível com reexportação)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Orientação: Horizontal (original) → Rotacionada 270° (alterado)
* Thumbnail: 3306 bytes (original) → 3335 bytes (alterado, recriada)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O conjunto **Progressive + 4:4:4 + ICC HP**, associado à alteração de orientação e ao aumento do tamanho do arquivo, caracteriza forte padrão de reprocessamento em Photoshop/similares. As mudanças são incompatíveis com fluxo direto de captura.

**Resultado: Provável Fraude** — **16 pontos** (nível **Muito Forte**).  
Os metadados são consistentes com reexportação por software de terceiros, combinando **Progressive + 4:4:4 + ICC HP.**

**Score de indícios:**

* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tamanho do Arquivo (variação relevante) → 1**
* **Miniatura (alterada/recriada) → 1**
* **Orientação → 1**

**subtotal (score bruto): 12**

**Ajuste qualitativo (Bônus de co-ocorrência)**

* **+2 Progressive + 4:4:4 em conjunto**
* **+2 ICC HP presente em conjunto com Progressive**

**Score final (bruto + ajuste): 16 — nível: Muito Forte**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A alteração da orientação, combinada com perfis ICC e Progressive, reforça a indicação de reexportação em software de edição. A análise visual deve ser usada como apoio, já que a rotação também pode alterar a percepção do documento.

# Nome da pessoa analisada: Guilherme

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão a redução significativa do tamanho do arquivo na versão alterada, a perda de resolução/dimensões originais, além de alterações no processo de codificação. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 409 kB → alterado 106 kB (redução significativa)
* Dimensões: original 1200×1600 px → alterado 600×800 px (redução de 75% na área)
* Processo de Codificação: Progressive DCT (original) → Baseline DCT (alterado)
* Subamostragem (YCbCr): mantida 4:2:0 em ambos
* ICC Profile: ausente em ambos (sem alteração).
* Orientação: Rotate 270° em ambos (mantida).
* Thumbnail: 4389 bytes (original) → 4696 bytes (alterado, recriada)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O padrão observado mostra **redução drástica de tamanho e resolução**, acompanhada de alteração no processo de codificação (Progressive → Baseline) e modificação na miniatura. Esses sinais indicam reprocessamento por software de terceiros.

**Resultado: Forte (suspeito)** — **9 pontos**.

**Score de indícios:**

* **Tamanho do Arquivo (redução significativa) → 1**
* **Dimensões (redução relevante) → 2**
* **Processo de Codificação (Progressive → Baseline) → 3**
* **Miniatura (alterada/recriada) → 1**

**subtotal (score): 7 — Forte (suspeito)**

**Ajuste qualitativo (Bônus de co-ocorrência)**

* **+2 Redimensionamento relevante + Processo de Codificação alterado**

**Score final (bruto + ajuste): 9 — nível: Forte**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A expressiva redução de resolução e tamanho de arquivo é indício claro de reprocessamento. A ausência de ICC ou metadados adicionais não descarta manipulação, já que a mudança no processo de codificação e a recriação da miniatura reforçam o padrão de edição.

# Nome da pessoa analisada: Janete

Identificada pelos **CPF: e RG: Não informado**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão a redução significativa do tamanho do arquivo na versão alterada, a perda de resolução/dimensões originais e ajustes nos parâmetros JFIF. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 117 kB → alterado 65 kB (redução significativa, ~45%)
* Dimensões: original 1080×679 px → alterado 800×503 px (redução relevante de resolução)
* Processo de Codificação: Baseline DCT em ambos (sem alteração)
* Subamostragem (YCbCr): mantida 4:2:0 em ambos
* ICC Profile: ausente em ambos (sem alteração).
* JFIF/Resolução: ausente no original → JFIF 1.01 com 96 dpi no alterado

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O padrão indica **reprocessamento simplificado**, com redução de tamanho e resolução e sobrescrita de parâmetros JFIF. Apesar de não incluir Progressive ou ICC HP, os sinais de perda de qualidade e alteração estrutural indicam manipulação digital.

**Resultado: Suspeita Moderada — 7 pontos (nível Suspeita Moderada).**Os metadados por si só sugerem apenas reexportação/redimensionamento**.**

**Score de indícios:**

* **Tamanho do Arquivo (redução significativa) → 2**
* **Dimensões (redução relevante) → 2**
* **Resolução/DPI (JFIF alterado) → 1**

**subtotal (score bruto): 5 — Baixo**

**Ajuste qualitativo (Bônus de co-ocorrência)**

* **+2 Redimensionamento relevante + Resolução JFIF alterada**

**Score final (bruto + ajuste): 7 — nível: Suspeita Moderada**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A forte redução de resolução e a sobrescrita de parâmetros JFIF, ainda que não acompanhadas de Progressive/ICC, constituem sinais de reexportação em software de terceiros.

# Nome da pessoa analisada: Patricia

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a alteração da subamostragem de cor, a inserção de perfil ICC Hewlett-Packard inexistente no original, bem como a presença de tags Adobe específicas de edição. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 257 kB → alterado 372 kB (aumento relevante)
* Processo de Codificação: Progressive DCT em ambos, mas no alterado há parâmetros adicionais de Photoshop
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Tags Adobe/Photoshop: presentes no alterado (APP14Flags, PhotoshopQuality, ProgressiveScans, ColorTransform)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

A versão alterada apresenta a tríade típica de reprocessamento em Photoshop: **Subamostragem 4:4:4 + ICC HP + Tags Adobe**, acompanhada de aumento de tamanho de arquivo. Esse conjunto é incompatível com captura original e caracteriza manipulação digital.

**Resultado: Provável Fraude — 17 pontos** *(nível Muito Forte).*

**Score de indícios:**

* **Tamanho do Arquivo (aumento relevante) → 1**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tags Adobe/Photoshop → 3**
* **Processo de Codificação (com Progressive e parâmetros Adobe) → 3**

**subtotal (score bruto): 13**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 Subamostragem 4:4:4 + Progressive**
* **+2 ICC HP + Tags Adobe**

**Score final (bruto + ajuste): 17 — nível: Muito Forte.**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

As tags Adobe e o perfil ICC Hewlett-Packard, em conjunto com subamostragem alterada, constituem assinatura clara de edição em Photoshop.

# Nome da pessoa analisada: “Jovem”

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão a redução significativa da resolução e do tamanho do arquivo, a alteração da subamostragem de cor, a inserção de perfil ICC Hewlett-Packard inexistente no original, bem como a presença de tags Adobe e registros específicos do Photoshop. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 91 kB → alterado 75 kB (redução significativa)
* Dimensões: original 720×1280 px → alterado 450×800 px (redução relevante de resolução)
* Processo de Codificação: Progressive DCT em ambos, mas no alterado há parâmetros adicionais do Photoshop
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Tags Adobe/Photoshop: presentes no alterado (APP14Flags, PhotoshopQuality, ProgressiveScans, IPTCDigest)
* Resolução/DPI (JFIF): 1 dpi (original) → 72 dpi no alterado

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O conjunto **4:4:4 + ICC HP + Tags Adobe/Photoshop + Redimensionamento** caracteriza fortemente reprocessamento em Photoshop/similares. As reduções de tamanho e resolução reforçam a incompatibilidade com captura direta de dispositivo.

**Resultado: Provável Fraude — 17 pontos *(nível Muito Forte).***

**Score de indícios:**

* **Tamanho do Arquivo (redução relevante) → 1**
* **Dimensões (redução relevante) → 2**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tags Adobe/Photoshop → 3**
* **Resolução/DPI (JFIF alterado) → 1**

**subtotal (score bruto): 13**

**Ajuste qualitativo (Bônus de co-ocorrência)**

* **+2 ICC HP + Tags Adobe/Photoshop em conjunto**
* **+2 Redimensionamento relevante + Subamostragem 4:4:4**

**Score final: 17 — Muito Forte (provável fraude)**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A análise visual do documento reforça os indícios técnicos, pois alterações de assinatura/elementos gráficos tendem a acompanhar esse padrão de metadados.

# Nome da pessoa analisada: Juliana

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a mudança no processo de codificação e a inclusão de perfil ICC Hewlett-Packard inexistente no original. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 184 kB → alterado 287 kB (aumento de 55%)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → sRGB IEC61966-2.1 (Hewlett-Packard) no alterado
* Thumbnail: 5211 bytes (original) → 5063 bytes (alterado, recompressão)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O padrão identificado (Progressive + 4:4:4 + ICC HP) caracteriza reprocessamento digital em Photoshop. O aumento do tamanho do arquivo e a alteração da miniatura reforçam a incompatibilidade com captura original.

**Resultado: Provável Fraude — 14 pontos *(nível Muito Forte).***Os metadados indicam reprocessamento digital com Progressive DCT + YCbCr 4:4:4 + perfil ICC sRGB/HP, ausentes no original.

**Score de indícios:**

* **Tamanho do Arquivo (aumento relevante) → 1**
* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Miniatura (alterada/recriada) → 2**

**subtotal (score bruto): 12**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 Progressive + Subamostragem 4:4:4**

**Score final: 14 — Muito Forte (provável fraude).**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A comparação visual deve ser utilizada como apoio, pois alterações na assinatura e elementos do documento reforçam os indícios técnicos de manipulação digital.

# Nome da pessoa analisada: Luan

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão o aumento do tamanho do arquivo na versão alterada, a alteração do processo de codificação, a mudança da subamostragem de cor e a inserção de perfil ICC Hewlett-Packard inexistente no original, além da presença de tags Adobe. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 185 kB → alterado 291 kB (aumento relevante)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 (original) → 4:4:4 (alterado)
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Tags Adobe/Photoshop: presentes no alterado (APP14Flags, ColorTransform)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

O conjunto de indícios **Progressive + 4:4:4 + ICC HP + Tags Adobe**, somado ao aumento de tamanho de arquivo, constitui assinatura clara de reprocessamento em Photoshop. Incompatível com fluxo original de captura.

**Resultado: Provável Fraude— 17 pontos *(nível Muito Forte).***Metadados indicam reprocessamento digital com Progressive DCT + YCbCr 4:4:4 + perfil ICC sRGB/HP e tags Adobe/APP14, ausentes no original.

**Score de indícios:**

* **Tamanho do Arquivo (aumento relevante) → 1**
* **Processo de Codificação (Progressive) → 3**
* **Subamostragem (4:4:4) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Tags Adobe/Photoshop → 3**

**subtotal (score bruto): 13**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 Progressive + Subamostragem 4:4:4 em conjunto**
* **+2 ICC HP + Tags Adobe em conjunto**

**Score final:** **17 — Muito Forte (provável fraude)**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**

A inserção simultânea de ICC Hewlett-Packard e Tags Adobe é um dos padrões mais consistentes de reprocessamento em Photoshop, reforçando a conclusão de manipulação.

# Nome da pessoa analisada: Lucas

Identificada pelos **CPF: e RG: Não informado.**

Observação: **Foram detectadas alterações nos metadados que indicam manipulação da imagem por programa de terceiros. Entre as divergências identificadas estão a mudança do processo de codificação, a inserção de perfil ICC Hewlett-Packard inexistente no original e a alteração de orientação. Esses elementos reforçam a hipótese de edição posterior em software de desktop (ex.: Photoshop).**

Pontos Importantes:

* FileSize: original 163 kB → alterado 148 kB (redução leve, ~9%)
* Processo de Codificação: Baseline DCT (original) → Progressive DCT (alterado)
* Subamostragem (YCbCr): 4:2:0 em ambos (sem alteração).
* ICC Profile: ausente no original → Hewlett-Packard sRGB IEC61966-2.1 no alterado
* Orientação: Rotate 90° (original) → Rotate 270° (alterado)
* Thumbnail: 5934 bytes (original) → 6247 bytes (alterado, recriada)

|  |  |
| --- | --- |
| Original | Alterada |
|  |  |
|  |  |

**Considerações finais:**

A presença simultânea de **Progressive + ICC HP**, associada à alteração de orientação e da miniatura, caracteriza padrão de reprocessamento em Photoshop.

**Resultado: Provável Fraude — 13 pontos (nível Muito Forte).**

**Score de indícios:**

* **Tamanho do Arquivo (variação leve) → 1**
* **Processo de Codificação (Progressive) → 3**
* **Perfis ICC (HP/Adobe) → 3**
* **Orientação alterada → 1**
* **Miniatura (alterada/recriada) → 1**

**subtotal (score bruto): 9**

**Ajuste qualitativo (Bônus de co-ocorrência):**

* **+2 Progressive + ICC HP em conjunto**
* **+2 Progressive + Miniatura alterada**

**Score final: 13 → Muito Forte (provável fraude)**

**Faixa de decisão:** 0–3 baixo / 4–7 Suspeita Moderada / 8–12 forte (suspeito) / **≥13 muito forte (provável fraude)**.

**Observação complementar (não pontuada):**O conjunto de ICC Hewlett-Packard e Progressive é um dos sinais técnicos mais consistentes de exportação em Photoshop, especialmente quando acompanhado de alterações de orientação e recriação de miniatura**.**

# Seção Final – Recursos e Padrões de Identificação

Links e Comandos Úteis.

* Ferramenta utilizada: ExifTool (Phil Harvey) - <https://exiftool.org/>
* Comando base para extração de metadados:
  + .\exiftool “C:\Folder\imagem.jpg”
* Comparação lado a lado de dois arquivos (exportando no formato json):
  + .\exiftool -a -G1 -s -json "C:\docs\brunaOriginal.jpg" -w %d%f.meta.json
  + .\exiftool -a -G1 -s -json "C:\docs\brunaFake.jpg" -w %d%f.meta.json

# Padrão de indícios de Manipulação em Metadados

Os itens abaixo sintetizam padrões recorrentes observados nas imagens classificadas como alteradas (fake), servindo de referência para triagem e auditorias futuras.

|  |  |  |  |
| --- | --- | --- | --- |
| **Categoria** | **Original (esperado)** | **Alterado (indício de fraude)** | **Observação** |
| **Tamanho do Arquivo** | Coerente com resolução e compressão | Aumento/redução significativa sem justificativa técnica | Reexportação/edição |
| **Processo de Codificação** | Baseline DCT (câmeras/dispositivos) | Progressive DCT | Indica reprocessamento |
| **Subamostragem de Cor** | YCbCr 4:2:0 | YCbCr 4:4:4 | Alteração comum em edições |
| **Perfis ICC** | Ausentes ou padrão da câmera/dispositivo | Hewlett-Packard / Adobe / Photoshop | Metadados não nativos adicionados |
| **Tags Adobe/Photoshop** | Inexistentes | APP14Flags, PhotoshopQuality, ColorTransform | Indicam exportação em software de edição |
| **Orientação (EXIF)** | Consistente com a captura | Divergente/modificada | Rotação artificial do arquivo |
| **Datas (Criação/Modificação)** | Campos coerentes entre si | Modify/Access divergentes da criação | Sinal de manipulação posterior |
| **Miniatura (Thumbnail)** | Tamanho consistente | Diferenças relevantes (maior/menor) | Exportação posterior detectada |
| **Resolução/DPI** | 72/96 dpi (comum) | 1 dpi ou variações incomuns | Reprocessamento ou conversão |

# Tabela – Pesos dos Indícios

|  |  |  |  |
| --- | --- | --- | --- |
| **Categoria** | **Força (nível)** | **Peso (1-5)** | **Observações de cautela** |
| **Tamanho do Arquivo** | Fraco | 1 | Varia com compressão, recorte, ruído, transporte. Nunca usar isolado. |
| **Processo de Codificação (Baseline/Progressive)** | Médio | 3 | Progressive pode vir de reexports legítimas. Mais forte se combinado com Subamostragem 4:4:4 ou APP14/Adobe. |
| **Subamostragem de Cor (YCbCr)** | Médio | 3 | 4:4:4 é incomum em câmeras. Aparece em Photoshop (com Progressive) e em Canva/Fotor. |
| **Perfis ICC** | Médio | 3 | Diferenciar: (a) genérico regravado = 2, (b) ausente = 3, (c) HP/Adobe = 3. Sozinhos são comuns, ficam fortes em conjunto. |
| **EXIF (Make/Model/ISO/etc.)** | Forte | 4 | Ausência total é sinal fortíssimo em Online/IA. Inconsistência (SceneType=Unknown no BeFunky) = 2. |
| **Tags Adobe/Photoshop (APP14, PhotoshopQuality, ProgressiveScans, XMP/IPTC)** | Médio | 3 | Típicos de Photoshop. Podem aparecer em reexports legítimas, mas juntos com Progressive/ICC são fortes. |
| **Software (campo, se explícito: Photoshop/Photopea/Canva/etc.)** | Forte | 4 | Indício direto de edição. “Confissão” do editor no campo Software/XMP. |
| **Software (campo vazio + EXIF ausente/ICC genérico)** | Médio | 2 | Padrão típico de editores online. Só vale quando acompanhado de outros sinais. |
| **Datas (CreateDate, DateTimeOriginal, ModifyDate)** | Médio | 3 | Incoerências são fortes indícios. Atenção a fuso horário ou cópias de arquivo. |
| **Miniatura (Thumbnail)** | Fraco → Médio | 2 | Diferença de tamanho de miniatura indica reexportação. Apoio, não decisivo isolado. |
| **Orientação (EXIF Orientation)** | Fraco | 1 | Alterações automáticas por apps de galeria são comuns. Só reforça em conjunto. |
| **Resolução/DPI (JFIF/EXIF)** | Fraco | 1 | Muitos apps fixam em 72 dpi. Irrelevante isolado. |
| **XMP/IPTC** | Médio | 2 | Gravações automáticas comuns em editores. Relevante quando aparecem sem EXIF ou junto com ICC/Adobe. |
| **Redimensionamento / Proporção** | Médio | 2 | Alterações grandes de resolução/proporção indicam reprocessamento. Ganham força com Progressive/ICC. |
| **Ausência de dados de câmera (Lens/Serial)** | Médio | 3 | Nem sempre presentes. Mais forte quando o fluxo deveria ter e sumiram. |
| **GPS / Geotag** | Fraco → Médio | 2 | Muitas imagens já não têm GPS. Só contar quando esperado (ex.: outros arquivos do lote têm). |
| **XMP / Tags de Software IA explícitas** | Muito Forte | 5 | Prova direta de IA. Exemplos: Edited with Google AI, compositeWithTrainedAlgorithmicMedia. |
| **C2PA / JUMBF Manifest (IA declarada)** | Muito Forte | 5 | Evidência inequívoca de processamento IA declarado/autenticado. Blocos criptográficos não podem surgir de captura nativa. |

**Regra de pontuação:**

1. Para cada indício presente, **some o “Peso (1–5)”** da tabela.
2. Aplique **bônus de co-ocorrência (+2 pontos cada)** quando houver as combinações abaixo (indicam reprocessamento típico):
   * **Progressive DCT + Subamostragem YCbCr 4:4:4**
   * **Perfis ICC HP/Adobe + Tags Adobe/Photoshop (APP14, PhotoshopQuality, ProgressiveScans, XMP/IPTC)**
   * **Datas incoerentes (CreateDate, DateTimeOriginal, ModifyDate) + (Progressive/4:4:4 ou ICC+Adobe)**
   * **Redimensionamento relevante + (Progressive ou Subamostragem 4:4:4)**
3. **Score final = Soma dos Pesos + Bônus de Combinações.**
   * Nenhum indício isolado “condena”; o valor está no **conjunto coerente**.
   * Aplicam-se as mesmas faixas de decisão da matriz:
     + 0–3 = Baixo (normal)
     + 4–7 = Suspeita Moderada
     + 8–12 = Forte (suspeito)
     + ≥13 = Muito Forte (provável fraude)

# Classificação por score

|  |  |  |
| --- | --- | --- |
| **Score final** | **Classificação** | **Ação sugerida** |
| **0 – 3** | **Baixo (normal)** | **Pode ser original ou reexportação legítima. Sem alerta.** |
| **4 – 7** | **Atenção (suspeita moderada)** | **Revisão humana/visual; solicitar arquivo de origem se necessário.** |
| **8 – 12** | **Forte (suspeito)** | **Reprovar ou exigir reenvio do original + justificativa de edição.** |
| **≥ 13** | **Muito Forte (provável fraude)** | **Recusa automática conforme política.** |

**Exemplo rápido**

* **Indícios: Progressive (3) + YCbCr 4:4:4 (3) + ICC HP/Adobe (3) + APP14/Photoshop (3) + Datas incoerentes (3)**
* **Soma dos Pesos = 15**
* **Bônus: Progressive+4:4:4 (+2), ICC+Adobe (+2), Datas+combo (+2) → +6**
* **Score final = 21 → Muito forte (provável fraude)**

# Resumo final

|  |  |  |
| --- | --- | --- |
| **Pessoa** | **Score final** | **Classificação** |
| **Adriana** | **13** | **Muito Forte (provável fraude)** |
| **Cristiano** | **17** | **Muito Forte (provável fraude)** |
| **Daniel** | **15** | **Muito Forte (provável fraude)** |
| **Djailson** | **16** | **Muito Forte (provável fraude)** |
| **Guilherme** | **10** | **Forte (suspeito)** |
| **Janete** | **7** | **(suspeita moderada)** |
| **Patrícia** | **17** | **Muito Forte (provável fraude)** |
| **Jovem** | **17** | **Muito Forte (provável fraude)** |
| **Juliana** | **14** | **Muito Forte (provável fraude)** |
| **Luan** | **17** | **Muito Forte (provável fraude)** |
| **Lucas** | **13** | **Muito Forte (provável fraude)** |