

APRESENTAÇÃO DE LAUDO PERICIAL

Processo: 00000000-09.2025.6.11.0000

Autor: Ministério Público do Estado de Algum Estado (MPAE)

Réu: Suspeito pelo crime de sequestro e cárcere privado

LAUDO PERICIAL

No dia 23 de abril de 2025, este Perito recebeu por **meios digitais oficialmente autorizados** a imagem em formato digital, apensada aos Autos do **Processo Judicial Hipotético 3**, cuja origem refere-se ao **Inquérito Policial 001/2017**, instaurado para apuração do crime de sequestro e cárcere privado, conforme denúncia oferecida pelo **Ministério Público de Algum Estado**.

Na sequência do trabalho pericial, no período de 24 de abril de 2025 a 22 de maio de 2025, em ambiente laboratorial (CyberOne – Laboratório de Computação Forense, Perícia Computacional e Inteligência Cibernética), este Perito realizou a análise técnica forense da referida imagem digital, a análise teve como finalidade responder aos quesitos formulados pela parte Autora.

No período de 23 a 27 de maio de 2025, este Perito elaborou o presente Laudo Pericial, descrevendo com verdade e com todas as circunstâncias o conjunto completo de informações que possa interessar ao Tribunal de Justiça de Algum Estado, no âmbito do processo em epígrafe. Todas as tarefas periciais foram realizadas em conformidade com o que preconiza a Lei No. 13.105, de 16 de março de 2015, em seu Artigo 473, do Código de Processo Civil, que, em suma, estabelece os parâmetros para elaboração de laudos periciais e pareceres técnicos periciais, que servem como diretrizes para o trabalho do Perito. A Computação Forense e a Perícia Forense Computacional consistem, basicamente, no uso de métodos técnicos e científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo. Este Perito observou o que preconiza a Norma ABNT ISO/IEC 27037:2013, que apresenta as diretrizes para identificação, coleta, aquisição, extração e preservação de evidências digitais em todas as etapas de um processo judicial e/ou de investigação, preservando, assim, a **cadeia de custódia**.

OBJETIVOS DA PERÍCIA

O trabalho pericial realizado por este Perito teve como objetivo geral a **análise técnica e forense da imagem digital** apresentada nos Autos do **Processo Judicial Hipotético 3**, a fim de verificar sua origem, autenticidade, integridade, possíveis alterações e elementos visuais presentes, conforme os quesitos formulados pela Parte Autora.

Este Perito aplicou técnicas e procedimentos típicos da Perícia Forense Computacional, com ênfase na análise técnica de arquivos de imagem digital, utilizando ferramentas especializadas para examinar a integridade do arquivo, os metadados (informações embutidas no arquivo digital que descrevem atributos técnicos, temporais e contextuais da imagem, como data de criação, resolução, software de câmera utilizada, entre outras informações técnicas que podem ser úteis em uma investigação), possíveis rastros de edição e elementos visuais presentes na evidência. Todo o processo foi conduzido com o que preconiza os princípios da cadeia de custódia, garantindo a preservação da evidência digital.

Na realização dos exames periciais, os seguintes objetivos específicos foram definidos e alcançados:

1. receber e preservar a evidência digital encaminhada (imagem em formato digital) por meios oficiais, assegurando sua integridade e autenticidade;
2. analisar tecnicamente a imagem digital, com a extração de dados estruturais e metadados, verificação de possíveis manipulações e identificação de elementos visuais relevantes à investigação;
3. correlacionar os elementos técnicos extraídos da imagem com os quesitos apresentados pela parte Autora, a fim de comprovar a participação do suspeito no crime;
4. elaborar e apresentar este laudo pericial.

OBJETOS PARA PERÍCIA

O material examinado por este Perito é composto pelo seguinte objeto digital:

1. Um arquivo, em formato **JPEG** (*Joint Picture Expert Group*), denominado **placaMoto.jpeg**, que foi apensado aos **Autos do Processo Judicial Hipotético 03** pela parte Autora – o Ministério Público de Algum Estado. Trata-se de uma imagem digital que registra o

possível suspeito conduzindo uma motocicleta próximo ao local do crime; A integridade do arquivo pode ser verificada, a qualquer tempo, pela HASH MD5 **D4233DB838CF71AAB9E1127A22E21803** e pela HASH SHA-256 **422F9D56432F14F0D07E26B6DF625447B41E6A9B77311CB8324E8E3C5913F8F9**;

QUESITOS

A parte Ré, através de seus patronos, não apresentou quesitos nos autos do processo. Os quesitos periciais (num total de 11 – onze), que deveriam ser analisados e respondidos por este Perito, foram apresentados pela parte autora – o **Ministério Público do Estado de Alagoas (MPAE)** – no documento **ID 987654321**.

METODOLOGIA

Na **primeira etapa do trabalho pericial**, este Perito realizou uma cópia do arquivo digital da imagem, para não correr o risco de comprometer o arquivo original durante as etapas a seguir, todas as análises foram realizadas em uma cópia idêntica do arquivo original, após realizar a cópia, este Perito verificou a integridade do arquivo de imagem, utilizando a ferramenta **HashCalc**, amplamente reconhecida no meio pericial para verificação de integridade da evidência digital, A análise foi conduzida em ambiente controlado, com objetivo de gerar os códigos HASH a partir dos algoritmos MD5 e SHA-256, a partir da evidência digital disponibilizada. Em seguida, os códigos gerados foram comparados com os valores previamente fornecidos nos autos, de forma a atestar se a integridade do arquivo foi mantida desde a sua aquisição, garantindo que o material a ser analisado não sofreu alterações durante sua cadeia de custódia. Os resultados dessa verificação estão documentados na sessão de resposta aos quesitos deste laudo.

Na segunda etapa do trabalho pericial, em ambiente laboratorial, este Perito procedeu com a extração e análise dos dados estruturais e metadados do arquivo de imagem. Utilizando o sistema operacional **Kali Linux**, reconhecido no meio da Computação Forense por dispor de ferramentas avançadas de análise digital. Foram utilizadas as ferramentas **mediainfo** e **exiftool** em linha de comando, ambas amplamente utilizadas em perícias digitais. A ferramenta **mediainfo** foi utilizada para extrair os dados estruturais da imagem, incluindo formato do arquivo, tamanho em bytes e resolução em pixels. E a ferramenta **exiftool** foi empregada para verificar a preservação dos metadados EXIF(*Exchangeable Image File Format*) e extraí-los, permitindo a identificação das

datas de modificação da imagem, bem como outros parâmetros técnicos relevantes para esta análise pericial.

Na terceira etapa do trabalho pericial, este Perito realizou a análise de autenticidade e detecção de adulterações na imagem digital. Para isto, utilizou-se ferramentas específicas de análise forense de imagens digitais, com o objetivo de identificar possíveis indícios de manipulação na imagem periciada. Para este propósito foram utilizadas as ferramentas de domínio público, **FotoForensics**(<https://fotoforensics.com/>) e **Forensically**(<https://29a.ch/photo-forensics/>), essas ferramentas utilizam algoritmos de detecção de inconsistências nos padrões de pixels da imagem, que possam indicar adulteração. Como última etapa da análise de adulteração, foi utilizado o software **JPEGSnoop** para uma análise profunda da estrutura da imagem, para identificação de compressões, editores utilizados e possíveis adulterações, com base na comparação com as assinaturas dos perfis de câmera e softwares de edição de imagem.

A combinação dessas ferramentas permitiu uma análise minuciosa dos elementos visuais e estruturais da imagem, fornecendo material para verificar a autenticidade desta evidência digital.

Na quarta etapa do trabalho pericial, este Perito realizou a melhoria da qualidade visual da imagem com o auxílio da ferramenta **ImageJ**, software amplamente utilizado em contextos forenses e científicos para análise, melhoria e medições precisas de conteúdo visual de imagens digitais. Foram aplicados filtros de ampliação, redução de ruído por movimento, contraste, brilho, nitidez e gamma para realçar a placa da motocicleta, no intuito de verificar a possibilidade de identificação da cadeia alfanumérica.

Na quinta etapa do trabalho pericial, este Perito utilizou novamente a ferramenta ImageJ, realizando a calibração de escala da imagem, tendo como referência as medidas reais da placa de uma motocicleta. Após a escala estar calibrada, foi possível utilizar a ferramenta de medição para estimar a altura do suspeito presente na imagem.

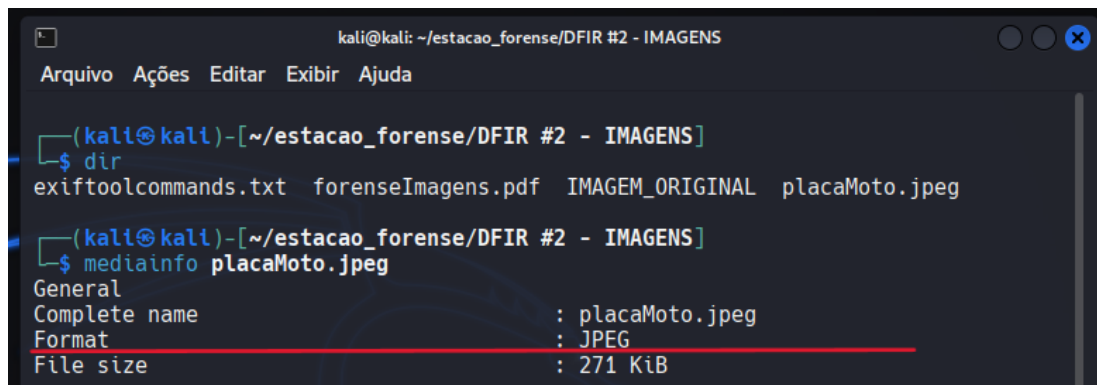
Na sexta etapa do trabalho pericial, este Perito elaborou este laudo e o entregou de forma eletrônica, via Plataforma Canvas, na seção Tarefas e no formato DOCX.

RESPOSTAS AOS QUESITOS

Realizadas todas as etapas do trabalho técnico, este Perito apresenta as respostas aos quesitos formulados e apresentados pelo **Ministério Público do Estado de Alagoas (MPAE)** no documento **ID 123456789**.

1. Qual o formato do arquivo da imagem?

Resposta: O formato do arquivo da imagem é formato **JPEG**, pelo fato do arquivo de imagem ter o tipo .jpeg, para conferir e confirmar isto, foi utilizada a ferramenta **mediainfo** em linha de comando, utilizando o comando “**mediainfo placaMoto.jpeg**” e analisar o dado “**Format**”, conforme mostra a **Figura 01**.



```
kali@kali: ~/estacao_forense/DFIR #2 - IMAGENS
Arquivo  Ações  Editar  Exibir  Ajuda

(kali@kali)-[~/estacao_forense/DFIR #2 - IMAGENS]
└─$ dir
exiftoolcommands.txt  forenseImagens.pdf  IMAGEM_ORIGINAL  placaMoto.jpeg

(kali@kali)-[~/estacao_forense/DFIR #2 - IMAGENS]
└─$ mediainfo placaMoto.jpeg
General
Complete name      : placaMoto.jpeg
Format              : JPEG
File size           : 271 KiB
```

Figura 01 – Imagem correspondente à extração dos dados estruturais, utilizando a ferramenta mediainfo, com destaque em “Format”

2. Qual é o código de integridade HASH MD5 e SHA-256 referentes ao arquivo de imagem?

Resposta: Ao utilizar a ferramenta **HashCalc**, foi constatado que os códigos **HASH MD5 e SHA-256**, referente a este arquivo de imagem são respectivamente: **D4233DB838CF71AAB9E1127A22E21803** e **422F9D56432F14F0D07E26B6DF625447B41E6A9B77311CB8324E8E3C5913F8F9**. Conforme mostra a **Figura 02**.

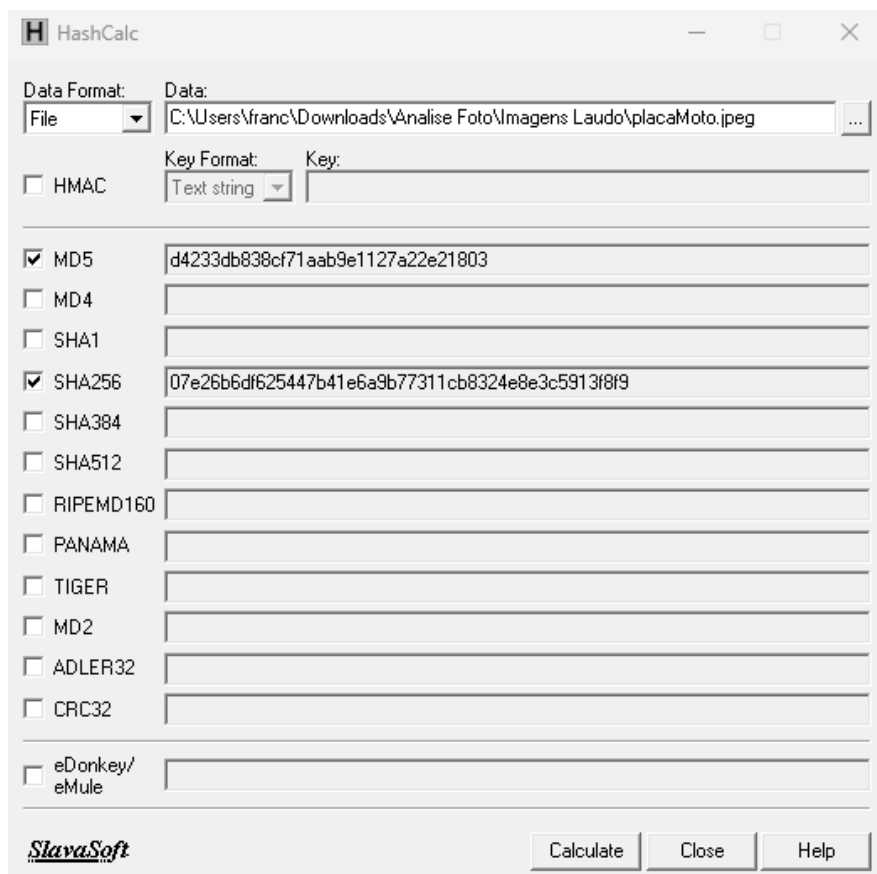


Figura 02 – Imagem da ferramenta HashCalc após calcular os códigos de integridade HASH com os algoritmos MD5 e SHA256

3. Qual é o tamanho do arquivo em Bytes?

Resposta: Ao analisar os dados estruturais com a ferramenta **mediainfo**, após verificar o dado **“File size”**, constatou-se que o arquivo de imagem possui um tamanho total de 271 KiB(*kibibyte*), conforme mostra a **Figura 03**, convertido para **Bytes** o tamanho é de **277.504**, pois cada KiB equivale a 1.024 Bytes.

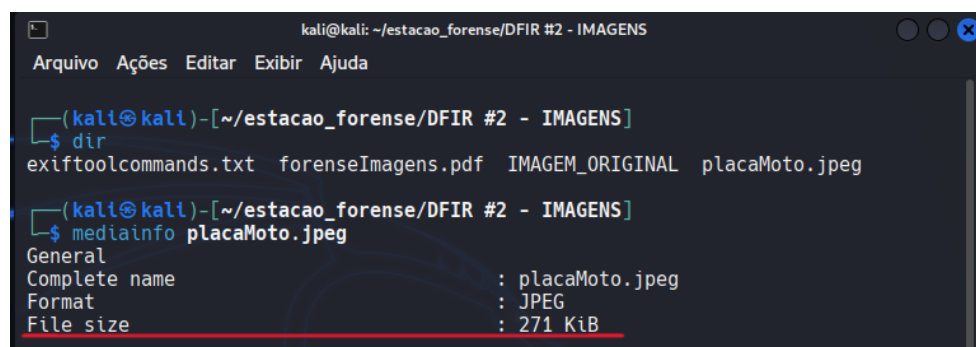


Figura 03 – Imagem correspondente à extração dos dados estruturais utilizando a ferramenta mediainfo, com destaque em “File size”

4. Qual é a resolução da imagem em pixels?

Resposta: Ao analisar novamente os dados estruturais extraídos pela ferramenta **mediainfo**, especificamente os dados “**Width**” e “**Height**” que correspondem a largura e altura em pixels, respectivamente. Dito isto, o tamanho em pixels deste arquivo de imagem, é de **1280 pixels de largura e 720 pixels de altura**, conforme mostra a **Figura 04**. Estas dimensões em pixels, correspondem a resolução **HD ou 720p**, que é um padrão muito utilizado em vídeos.

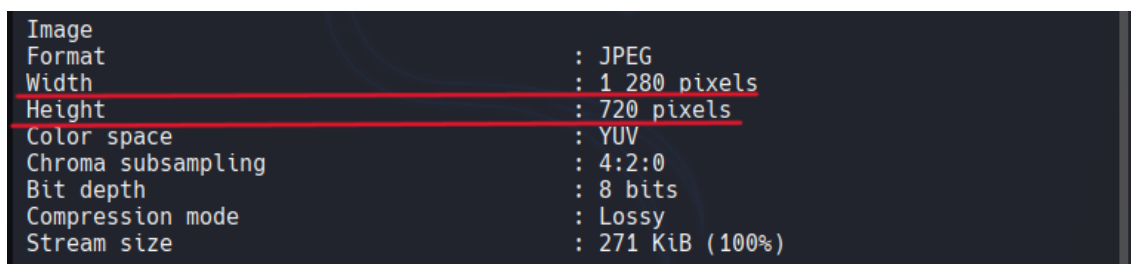


Image	
Format	: JPEG
Width	: 1 280 pixels
Height	: 720 pixels
Color space	: YUV
Chroma subsampling	: 4:2:0
Bit depth	: 8 bits
Compression mode	: Lossy
Stream size	: 271 KiB (100%)

Figura 04 – Imagem correspondente à extração dos dados estruturais utilizando a ferramenta mediainfo, com destaque em “Width” e “Height”

5. Qual é a data e horário de criação do arquivo de imagem?

Resposta: Utilizou-se a ferramenta **exiftool** em linha de comando, para extrair os metadados do arquivo de imagem. Porém, não foi encontrado nenhum metadado correspondente a data e horário de criação deste arquivo, este metadado pode ter sido perdido durante o envio da referida imagem ou removido para ocultar essa informação.

Mas ao analisar os **elementos visuais** da imagem, verificou-se que no canto superior direito possui uma data e hora, conforme mostra a **Figura 05**, indicando que a imagem foi retirada da gravação de uma câmera de segurança. A data e hora correspondem ao dia **12 de janeiro de 2017 às 10h 40min e 39s**.



Figura 05 – Imagem do canto superior do arquivo de imagem periciada, com a marcação da data e hora em que essa imagem foi capturada

6. Qual é a data e horário da última modificação no arquivo de imagem?

Resposta: Ao analisar o arquivo metadados.txt, que contém os metadados extraídos na ferramenta **exiftool**, utilizando o comando **“exiftool -e placaMoto.jpeg > metadados.txt”**, este comando faz a extração dos metadados para um arquivo de texto. Após extrair os metadados, constatou-se a existência do metadado que exibe a última modificação feita no arquivo de imagem, com data e hora sendo no dia **17 de junho de 2025 às 11h 19min e 14s**, conforme mostra a **Figura 06**.

```

1 ExifTool Version Number      : 13.10
2 File Name                    : placaMoto.jpeg
3 Directory                    : .
4 File Size                    : 277 kB
5 File Modification Date/Time  : 2025:06:17 11:19:14-03:00
6 File Access Date/Time       : 2025:06:22 20:57:13-03:00
7 File Inode Change Date/Time  : 2025:06:22 20:57:13-03:00
8 File Permissions             : -rw-rw-r--
9 File Type                    : JPEG
10 File Type Extension         : jpg
  
```

Figura 06 – Imagem correspondente à extração dos metadados utilizando a ferramenta exiftool, com destaque em “File Modification Date/Time”

7. Há sinais de edição e/ou adulteração no conteúdo do arquivo de imagem?

Resposta: Ao utilizar as ferramentas de domínio público **Forensically** e **FotoForensics** para verificar se a imagem possui pixels adicionados, não foi encontrado nenhum sinal de manipulação ou edição do conteúdo visual desta imagem digital. Porém ao utilizar o software **JPEGsn00p**, o arquivo foi classificado como **“Class 1 – Processed/Edited”**, como mostra a **Figura 07**, indicando

alto grau de probabilidade de ter sofrido alguma alteração, foram encontradas assinaturas de software de edição, mas como não foram identificadas alterações visuais na referida imagem, estes softwares foram utilizados para modificar ou remover metadados e comprimir a imagem digital, portanto **há indícios de adulteração** neste arquivo e o mesmo não se trata do registro original.

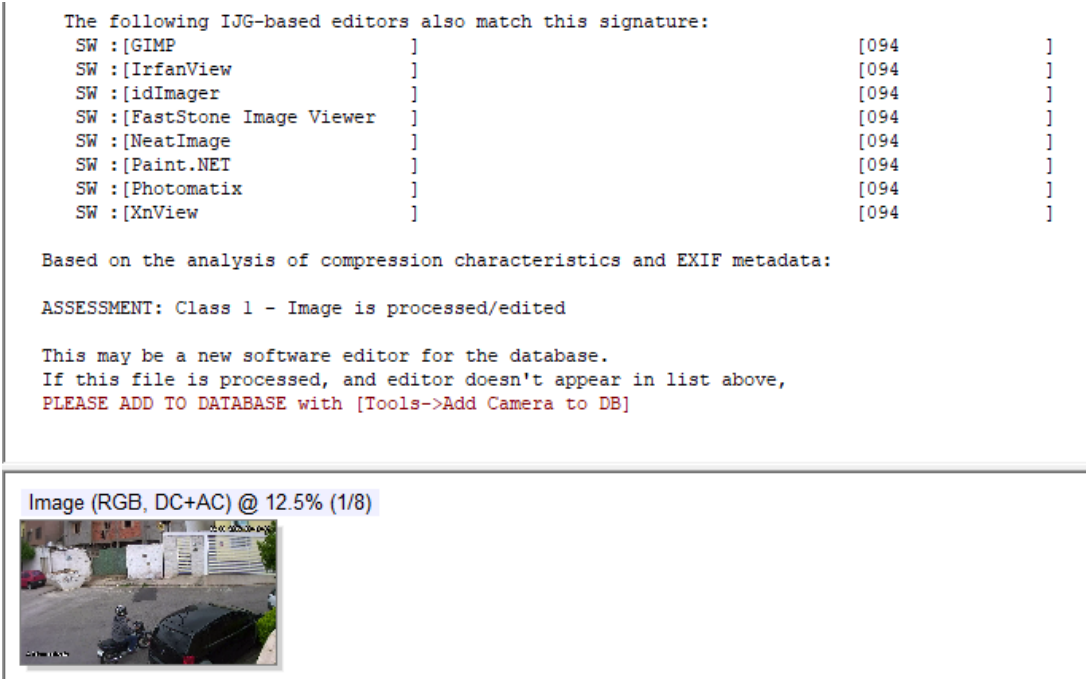


Figura 07 – Imagem correspondente ao resultado da análise de adulteração no software JPEGsnoop

8. Os metadados da imagem foram preservados? Em caso afirmativo, apresente os metadados extraídos do arquivo de imagem.

Resposta: Através do resultado da extração de metadados utilizando a ferramenta **exiftool**, pode-se afirmar que os principais metadados foram preservados, como data e hora da última modificação, resolução da imagem, método de compressão utilizado, tipo de câmera que foi utilizada para a captura deste arquivo de imagem, entre outros. Todos os metadados extraídos estão apresentados a seguir:

ExifTool Version Number	13.10
File Name	placaMoto.jpeg
Directory	.
File Size	277 kB
File Modification Date/Time	2025:06:17 11:19:14-03:00

File Access Date/Time	2025:06:22 20:57:13-03:00
File Inode Change Date/Time	2025:06:22 20:57:13-03:00
File Permissions	-rw-rw-r--
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
JFIF Version	1.01
Resolution Unit	inches
X Resolution	96
Y Resolution	96
Exif Byte Order	Big-endian (Motorola, MM)
Orientation	Horizontal (normal)
Image Width	1280
Image Height	720
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

9. É possível identificar a placa da motocicleta? Em caso afirmativo, qual é a placa?

Resposta: Utilizando o software **ImageJ** para aplicar filtros e melhorias na imagem digital, no intuito de conseguir identificar a cadeia alfanumérica da placa, foi realizada a aplicação do plugin *Projective Mapping*, no intuito de corrigir a perspectiva da placa, em seguida, foi utilizado o plugin *Motion Deblur*, para corrigir o desfoque por movimento, por fim, foram aplicadas edições no brilho, contraste e *gamma* da imagem para a melhor visualização possível, conforme mostra na **Figura 07**. Com as melhorias, foi possível identificar com certeza, 2 (duas) das 3 letras e 3 (três) dos 4 números, sendo **E Y 1 3 0**.

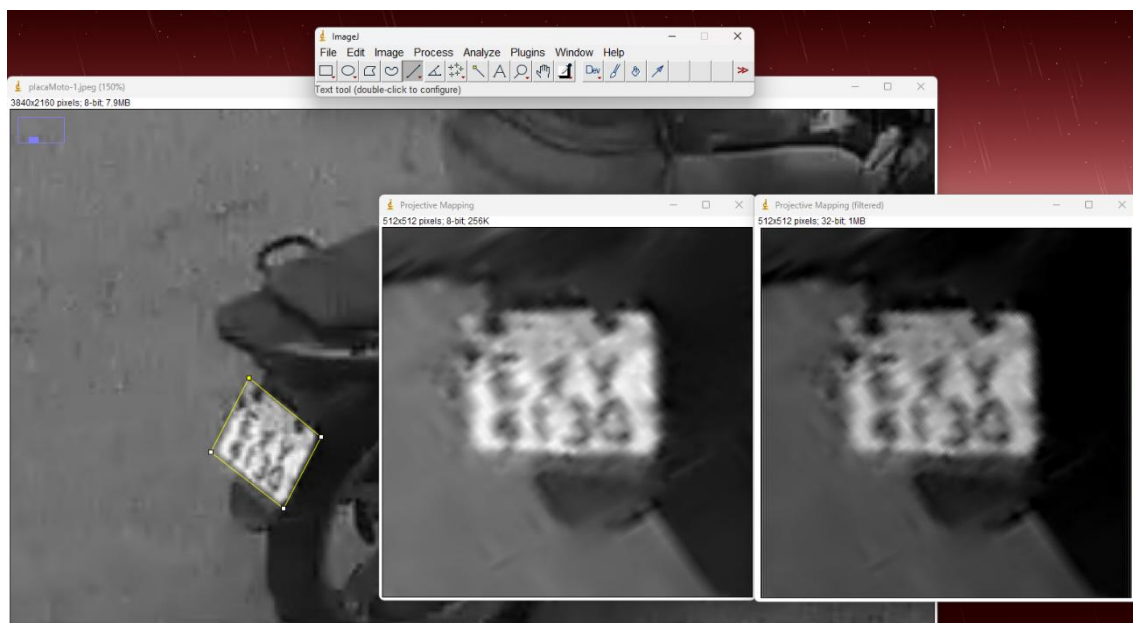


Figura 07 – Imagem da placa na ferramenta ImageJ após as melhorias aplicadas

10. Caso a placa tenha sido identificada, é possível informar outros dados sobre o veículo?

Resposta: Como os caracteres alfanuméricos referente à placa não foram totalmente identificados com clareza, não foi possível utilizar ferramentas que verificam dados sobre o veículo através da placa.

11. É possível estimar a altura do(a) condutor(a) da motocicleta? Em caso afirmativo, qual é a altura estimada?

Resposta: Baseando-se na medida da placa da motocicleta que possui 20cm de comprimento, foi possível calibrar o **ImageJ** com esta medida, assim conseguindo realizar uma medição e estimar a altura do suspeito, alcançando a estimativa de **1,77cm** de altura.

CONCLUSÃO

No período de realização da presente análise pericial, entre os dias de 24 de abril de 2025 a 22 de maio de 2025, este Perito realizou a verificação técnica do arquivo de imagem denominado **placaMoto.jpeg**, por meio do emprego de ferramentas consagradas na área de informática forense, como **Mediainfo**, **Exiftool**, **HashCalc**, **JPEGsnoop**, **Forensically**, **FotoForensics** e **ImageJ**.

As análises permitiram responder de forma fundamentada aos quesitos apresentados, abrangendo informações relativas ao formato, integridade, tamanho, resolução, datas relevantes, preservação de metadados e possibilidade de adulteração.

Constatou-se que o arquivo está em formato JPEG e possui os códigos de integridade HASH MD5 e SHA-256, garantindo autenticidade quanto à cópia periciada. Foi possível determinar o tamanho do arquivo em bytes e sua resolução, bem como a data e hora da última modificação do arquivo.

Verificou-se que os metadados principais foram preservados, mas a análise com o software **JPEGSnoop** apontou indícios de alteração, classificando o arquivo como “**Class 1 – Processed/Edited**”, possivelmente em função de processos de recompressão ou modificação de metadados, corroborando que o arquivo analisado **não corresponde ao registro original**, ainda que não tenham sido identificadas alterações visuais no conteúdo da imagem.

A análise visual com aprimoramento por filtros permitiu identificar parcialmente os caracteres da placa da motocicleta como **E Y 1 3 0**, entretanto, não foi possível obter todos os caracteres para identificação plena do veículo. Por fim, a estimativa da altura do condutor, com base na calibração da medida da placa, indicou aproximadamente **1,77 metros de altura**.

Foram estes os elementos analisados, periciados e passíveis de serem apresentados por este Perito. Nada mais havendo a constar, este Perito encerra o presente Laudo Pericial, elaborado em 12 (doze) páginas.

Poços de Caldas – MG, 27 de maio de 2025.

Bruno Felipe Barretto de França

Estudante do 4º Período de Ciência da Computação | Perito Judicial

Sobre o Perito (conforme preconiza o inciso II, § 2º do artigo 465 do CPC)

Bruno Felipe Barretto de França, Estudante de Ciência da Computação

Em 2023 iniciou o Curso de Ciência da Computação da Pontifícia Universidade Católica de Minas Gerais – PUC Minas (www.pucpcaldas.br), campus de Poços de Caldas, e encontra-se no 4º período do curso.