

# ARGO-FIAS

**ARGO-FIAS** segue as diretrizes da NIST SP 800-86 para apreciação, análise e relatórios. Todos os métodos incorporados são validados cientificamente e todo o fluxo de trabalho é documentado automaticamente.

**ARGO-FIAS** é um pacote de software fácil de usar que oferece técnicas de análise e autenticação de imagem forense em um ambiente prático. Hoje, a manipulação de imagens tornou-se muito mais sutil, fácil e generalizada com o advento de software com ajustes de edição de imagem, como a adição de camadas, a remoção de conteúdo e a clonagem de objetos. Se a imagem foi manipulada por motivos de publicação ou para ofuscar informações, o ARGO-FIAS é a solução completa para os desafios de autenticação de imagem mais complexos.

**ARGO-FIAS** oferece ferramentas para análise global, local e PRNU: **Structure** (estrutura) executa a análise da estrutura do arquivo para detectar inconsistências ou vestígios de dados extras ocultos no arquivo de evidências

**EXIF** extrai as informações de EXIF e Metadados

**JPG QT** extrai as tabelas de quantificação JPG e as compara automaticamente em vários bancos de dados

**JPG DCT** extrai e traça os coeficientes de CA e DC da transformada discreta de cossenos (DCT) do JPG

**CLA** analisa o nível de compressão da imagem de evidência

**CFA** exibe a análise da matriz de filtros de cores da imagem de evidência

**Color spaces** (espaço de cores) divide a imagem de evidência nas camadas de espaço de cores principais (por exemplo, RGB, CMYK, HSL)

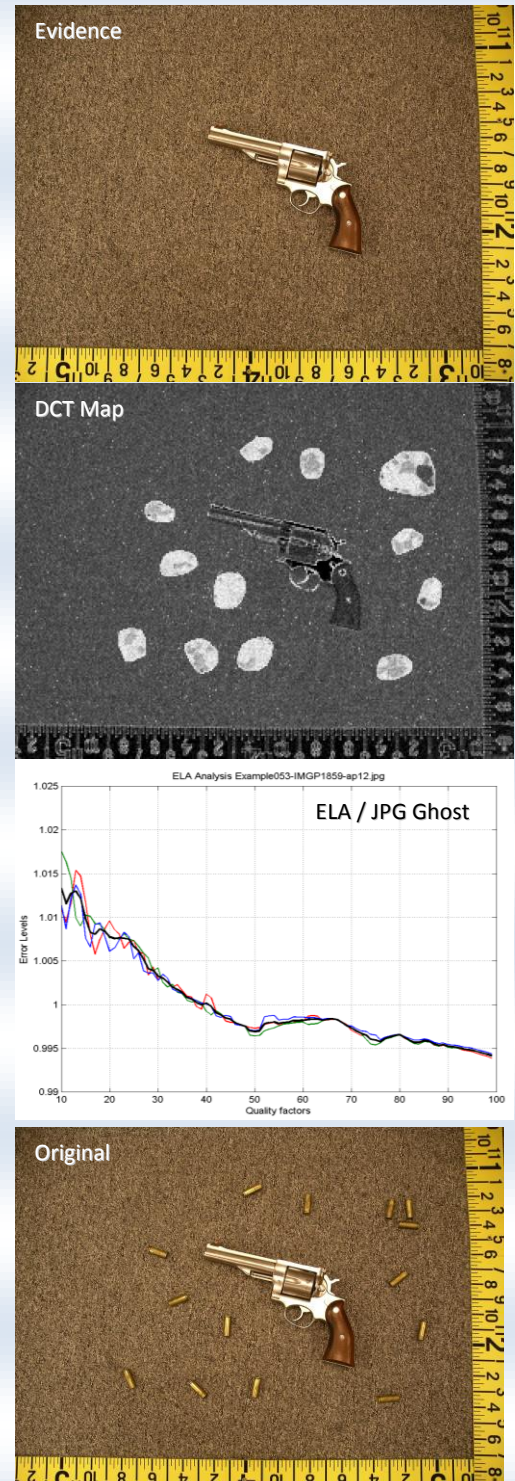
**Mapa DCT** calcula e exibe o mapa da transformada discreta de cossenos

**ELA** usa análise de nível de erro para detectar vestígios de manipulação local e para investigar o histórico de compressão do arquivo de evidências (JPG Ghost)

**Probability Map** mostra o mapa de probabilidades da imagem de evidência

**Correlation Map** aplica correlação de nível de pixel para detectar traços de manipulação local

**Block Analysis** (análise de bloco) usa algoritmos de nível de bloco para detectar vestígios de manipulação





**Hist Eq** aplica equalização de histograma por cada camada

**High Pass** aplica um filtro passa-alto na imagem de evidência

**PRNU Map** permite ao usuário extrair e analisar vários mapas de não-homogeneidade de resposta da foto

**2D DFT** executa uma transformada rápida de Fourier bidimensional da imagem de evidência

**Clone Detect** procura por traços de função de clone, ou copiar/colar, dentro da mesma imagem

**(-) CC MQD** calcula a diferença matemática, correlação e diferença quadrática média entre evidência e uma imagem de referência do mesmo tamanho

**PRNU Median** usa o método de filtro de mediana para extrair a não-uniformidade de resposta da foto e compará-lo contra um modelo de referência de uma câmera conhecida

**PRNU Wavelet** usa o método Wavelet para extrair a não-uniformidade de resposta da foto e compará-lo com um conjunto de imagens de referência de uma câmera conhecida e um banco de dados incorporado; os resultados são relatados como razões de verossimilhança (RV)

**Average** (média) calcula e salva a imagem média de todos os arquivos de imagem de uma pasta

**File Batch** (lote de arquivo) permite aos usuários processar um arquivo em lote

**Folder Batch** (lote de pasta) processa toda a pasta de imagens de evidências

**Fast Folder Batch** permite aos usuários uma análise rápida executando apenas Structure, EXIF e JPG QT na pasta de imagens de evidências

**Archive Case** Criará um arquivo ZIP contendo a evidência e todos os resultados da análise, e um relatório HASH será gerado. Archive Case será executado automaticamente durante um lote de Arquivo ou Pasta.

**ARGO-FIAS** também detecta e extrai (com base em esculpimento forense) o Thumbnail (miniatura) e Preview (prévia) de JPGs e gera um relatório de Análise Hex para futuras investigações hexadecimais do arquivo de evidências.

Observe que o **ARGO-FIAS** é um sistema forense que protege seus arquivos e trabalhos de casos de acordo com as melhores práticas para laboratórios de provas digitais, de modo que nenhuma conexão com a Internet e redes sociais, mapas, mecanismos de busca de imagens ou outros serviços on-line são solicitados ou permitidos.

**ARGO-FIAS** foi testado e instalado com sucesso no Windows XP, 7 e 8 de 32/64 bits. A configuração recomendada é processador: i7, 16 GB de RAM, 512 GB HDD (estado sólido preferido).