Perícia Computacional em Metadados de Imagens

Em um episódio ocorrido na Internet, uma personalidade disponibilizou em seu site imagens com "crop" apenas em seu rosto, para que somente tal área fosse exibida. Crackers então obtiveram acesso ao metadado .db que indexa e gerencia as imagens para o "preview", onde havia o link para o arquivo original. Moral da história? As fotos "nua de corpo inteiro" circularam pela Internet, causando certos constrangimentos à celebridade.
(http://graphicssoft.about.com/b/2003/07/26/techtvs-cat-schwartz-exposed-is-photoshop-to-blame.htm)
Thumbnails são arquivos que indexam as imagens, além exibir, em alguns padrões, uma versão "miniatura" da mesma. Segundo a sábia Wikipédia, "Thumbnails são versões reduzidas de imagens, usadas para tornar mais fácil o processo de as procurar e reconhecer. Os motores de busca de imagem e programas de organização destas os usam muitas vezes, tal como alguns sistemas operativos e ambientes de trabalho modernos, como o Windows XP, KDE e o GNOME"

Já softwares como Photoshop e PhotoPaint arquivam no próprio arquivo original uma "versão" em miniatura da imagem. O problema ocorre na atualização da miniatura, quando o original é modificado ou ajustado para ser exibido ao público. Hoje, na Internet, é possível encontrar centenas de Softwares que geram Thumbnail das imagens, como em http://baixaki.ig.com.br/download/Thumbnail-Generator.htm.

Além dos Thumbs, imagens contém metadados EXIF. EXIF (Exchangeable Image File Format) são informações gravadas nas próprias fotos no momento em que ela é tirada ou editada. Existem dezenas de programas que exploram tais informações como Wexif, ActiveMetaData, etc. Em EXIF.org (http://www.exif.org/samples.html) é possível conhecer imagens e máquinas digitais que geram EXIFs, bem como programas para

explorá-los.

A questão da exploração indevida de thumbnails é polêmica. Nos Estados Unidos, em recente caso Kelly v. Arriba Soft Corporation, travou-se uma ardente discussão sobre o uso indevido de thumbnails e fair use (uso justo de direitos autorais e da imagem). Em primeira instância a Ré foi condenada infratora por ter utilizado thumbnails que faziam referências aos originais em seu motor de busca. Porém, em segunda instância, na Corte de Apelações, decidiu-se que os thumbnails não eram ilegais. Porém uma coisa é linkar thumbnails, e a outra é a exploração para verificar como era a imagem original.

Dentre os Softwares utilizados para visualizar e gerar thumbnails está o Infran View (http://www.irfanview.com/). Mas você ainda acredita que suas imagens, após deletadas, são irrecuperáveis. Então faça um teste: Digite na Pesquisa do Windows: thumbs.db.

Quando você visualiza imagens e vídeos em miniatura, o Sistema Operacional cria arquivos ocultos nas pastas, chamados de thumbs.db. Tais arquivos são considerados Alternate Data Stream, então se não os localizar, altere as configurações de exibição de arquivos do seu Explorer. Eles também são gerados naquele pendrive ou dispositivo que você empresta para amigos e colegas. Como dito, alguns programas de edição, em simples crop (efeito recortar do Photoshop), não atualizam os metadados, então, as conseqüências podem ser catastróficas, como no exemplo abaixo:

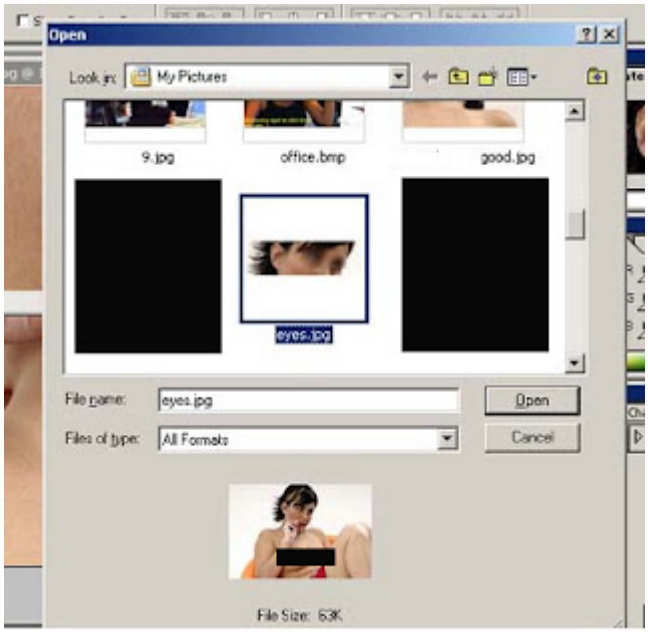


Imagem cropada e substituída, porém sem atualização de thumbnail. Ao se exibir a imagem cropada em miniatura, é possível verificar a versão original da imagem.(Fair use)

Existe porém a possibilidade de não gerar miniaturas no sistema Windows:

1. No Windows Explorer clique em Ferramentas. 2. Escolha Opções de pasta.3. Escolha Modo de exibição.4. Marque um x em Não armazenar miniaturas em cache. 5. Clique em Aplicar a todas as pastas. 6. Clique em Aplicar e em OK.

Outra técnica é zerar as primeiras 10 posições (bytes) em hexadecimal da imagem. Na maioria dos casos, as alterações na imagem são mínimas, porém o resultado é alcançado, ou seja, o Photoshop não processa os bytes alocados para o Thumbnail. (Atenção em alguns padrões isso pode corromper o arquivo).

Deixando as técnicas de eliminação de lado, falamos de aplicações extremamente úteis na recuperação de imagens que um dia existiram na máquina, por meio de seus thumbs persistentes no sistema.

Não só os thumbs dos sistemas de imagens merecem cuidados mas os “crops” existentes em blogs, fóruns e sites de relacionamento. Em um outro caso em que presenciamos, uma

mulher noiva inseriu uma foto com um ex-namorado em um blog e recortou (“crop”) mantendo somente seu rosto. Não durou muito para descobrirem a imagem original por trás da camada de ilusão do crop. A imagem chegou até o e-mail do então noivo (!)

O WFA (http://www.mitec.cz/wfa.html) é um utilitário forensics que pode rasterar uma imagem iso ou dd em busca de thumbnails e então extrair as minituras existentes. Talvez poderemos não ter tudo, mas o suficiente e com ética.

Muito comum em computação forense, a recuperação de arquivos, porém, como bits significantes já foram realocados com novas informações, a imagem recuperada apresenta-se corrompida total ou parcialmente. Abaixo podemos visualizar um exemplo de arquivo corrompido, mas que preserva seu thumb intacto (Baixe a imagem para testes forenses em http://www.legaltech.com.br/corrompida_milagre.jpg):

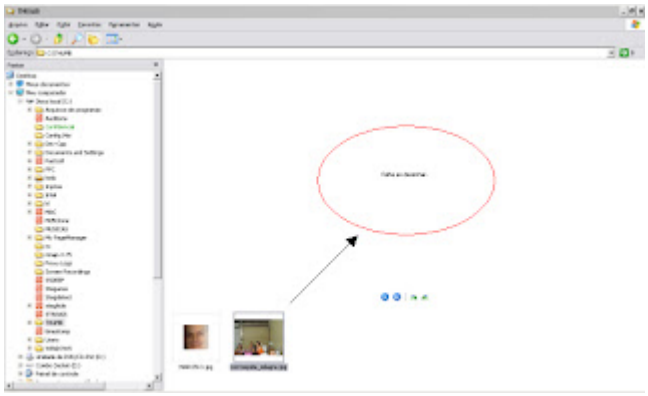
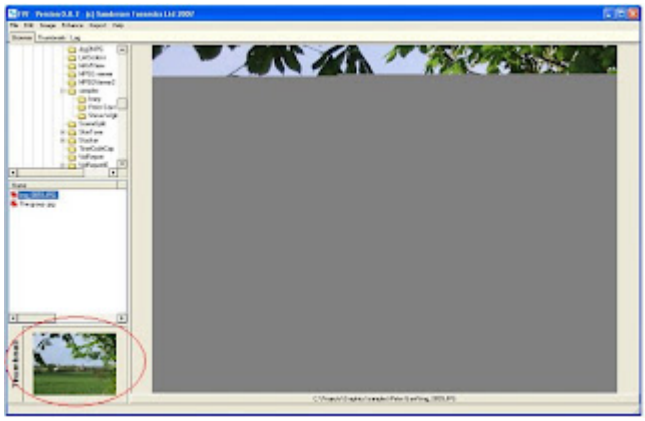


Imagem corrompida_milagre.jpg recuperada pelo ext2recover. Falha ao processar o arquivo, mas o thumb é visível.

Porém há casos em que a miniatura foi prejudicada. Em tal cenário, uma ferramenta forense pode auxiliar a reconstruir o passado com base nos fragmentos da miniatura. O Software Forensic Image Viwer (http://www.sandersonforensics.com/content.asp?page=103) é uma ferramenta capaz de analisar diretórios e imagens corrompidas, encontrando thumbnails embutidos em certos formatos de imagens e rastreando dados EXIF embutidos.

No exemplo abaixo, uma imagem corrompida, porém foi possível extrair metadados envolvendo sua miniatura, que estava íntegra:



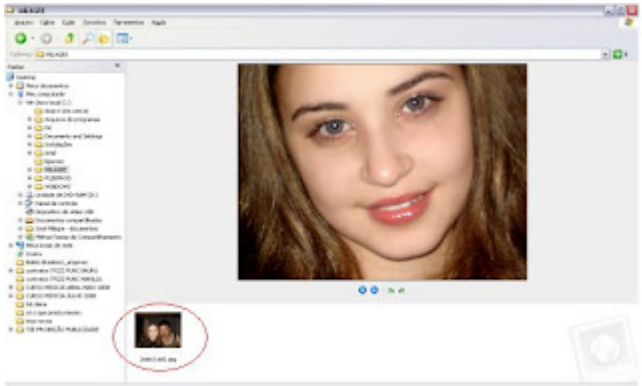
Screen de recuperação de metadados de imagens por meio do FIV

Outra excelente ferramenta é para recuperação de metadados de imagens excluídas é o Vinetto (http://vinetto.sourceforge.net/). Vinetto é um binário forense utilizável por linha de comando, cuja função é analisar arquivos .db em partições FAT32 e NTFS. A explicação é simples: Quando uma imagem é deletada, seu thumbnail relativo e demais metadados permanecem armazenados no arquivo Thumbs.db. Então, os dados contidos nestes thumbs podem revelar quais imagens existiram na máquina, sendo um dado útil ao profissional de investigação computacional. O Vinetto extrai as informações dos arquivos thumbs.

Ainda, para manipulação de headers EXIF das imagens, recomendamos aos profissionais de perícia forense a utilização da ferramenta JHEAD.exe (http://www.sentex.net/~mwandel/jhead/). Tal ferramenta, disponível para Windows e Linux, é essencial para um perito, podendo precisar data e hora em que a foto foi tirada, máquina e modelo (embora uma investida hexadecimal possa revelar tal dado), distância do fotógrafo e fotografado, se utilizou flash ou não, além poder realizar um wipe (esterilização) em timestamps e replace (sobrescrição) em cabeçalhos e informações EXIF.

Jhead em ação: Informações extraídas de uma imagem .jpg

Como constatado, informações thumbnails e EXIFs podem persistir em um sistema mesmo após a exclusão das imagens. Em tal cenário, a perícia pode se valer da recuperação de arquivos thumbs e posteriormente de analisadores e recuperadores de metadados em tais arquivos. Deve-se ter em mente porém que alguns padrões de sistemas operacionais e softwares de edição não sobrescrevem as informações dos thumbs em pequenas alterações na imagem, ou na aplicação de efeitos blur (para embaçar a imagem) ou crop (cortar o arquivo preservando seu nome e dados). Assim, em uma simples análise da Película ou miniatura do arquivo, é possível identificar o arquivo original, posteriormente editado:



Arquivo editado mas que preservou o thumbnail original.

Concluindo, procuramos no presente trabalho demonstrar como as informações relativas a imagens podem persistir mesmo após a eliminação das mesmas. As técnicas apresentadas podem ser úteis ao perito em processos envolvendo difamação, incitação,

pornografia infantil, dentre outros delitos praticáveis pela Rede Mundial de Computadores. Recomenda-se, sempre realizar os testes na imagem do disco, de maneira a preservar a identidade original dos dados obtidos. Para fazer o teste da miniatura acima, faça o download da imagem a seguir, e exiba no Windows Explorer em "Película" (http://img517.imageshack.us/img517/3368/2eds11zid1.jpg).

Até a próxima.