FIAP ON

BIOHACKING,
DEEP WEB E CRIPTOGRAFIA

ESTEGANOGRAFIA

ALESSANDRO VINÍCIUS VIEIRA

6

LISTA DE FIGURAS

SUMÁRIO

6 ESTEGANOGRAFIA

6.1 Introdução

Por diversos momentos Hollywood tentou demonstrar a vida de espiões em suas “missões impossíveis” ao redor do mundo. Porém diferente das telas de cinema, onde espiões usam complexos gadgets de comunicação criptografada, na vida real são técnicas simples como a esteganografia que permitem o envio e recebimento de mensagens confidenciais entre agentes de inteligência.

Para e pense um pouco… você já viu algum perfil no Twitter ou Instagram que, apesar de não ter muitas (ou quase nenhuma postagem), além de ter pouquíssimos seguidores, possui algumas fotos “sem sentido” postadas? Pois é, pra você pode não parecer ter muito sentido mas com certeza existe algum destinatário que entende muito bem o conteúdo destas imagens. E quando digo conteúdo, não me refiro ao que conseguimos ver nestas imagens...

6.2 O que é a Esteganografia?

Segundo Vicentini et. al. (2017), esteganografia é uma palavra de origem grega, na qual *stegano* significa “escondido ou secreto” e *grafia*, “escrita ou desenho”. Diferentemente da criptografia, que esconde o conteúdo de mensagem a tornando ilegível, a esteganografia obscurece a existência de informação, ocultando-a.

Uma mensagem ocultada por meio de técnicas esteganográficas não atrai atenção para si mesma, para o transmissor ou para o receptor. Uma das formas básicas de técnicas de esteganografia, é a alteração do bit menos significativo, que não afeta a visualização da imagem final.

Ainda conforme Vicentini et. al. (2017) a técnica de esteganografia tem sido utilizada desde a Antiguidade, quando se desejava encaminhar mensagens escondidas. A primeira utilização confirmada da técnica pode ser encontrada em “As Histórias” de Heródoto, a qual descreve no século V a.C. que um tirano grego foi aprisionado por um rei. O tirano queria fazer contato secreto com seu superior.

Assim, escolhendo um escravo fiel, que servisse de intermediário, raspou sua cabeça e, em seu couro cabeludo, foi feita uma tatuagem com uma mensagem que seria enviada ao superior. O escravo fiel aguardou seu cabelo crescer e posteriormente foi enviado até o superior com a instrução de raspar novamente seus cabelos para que a mensagem enfim fosse lida.

Com o desenvolvimento da tecnologia, a esteganografia foi aplicada no ambiente computacional a fim de mascarar dados sem detecção por seres humanos.

Um exemplo básico da aplicação da técnica, é a inserção do dado em um objeto cobertura, que produz a ocultação, então a chave estego controla todo o processo restringindo a recuperação e ou detecção do dado inserido.

Porém, assim como foram desenvolvidas ferramentas para criar a camuflagem, existe a esteganálise, que recupera textos, imagens, vídeos ocultos em objeto cobertura.

6.3 Aplicação da esteganografia em imagens

De acordo com Vicentini et. al. (2017), a utilização de esteganografia com auxílio de software abrange diversos métodos para ocultação de dados. São eles:

a) De acordo com Rocha (2003), Least Significant Bit (LSB) baseia-se em modificar os bits menos significativos de cada pixel (menor unidade da imagem digital), camuflando, assim, informações. A forma de inserir dados com o LSB seria da seguinte maneira:

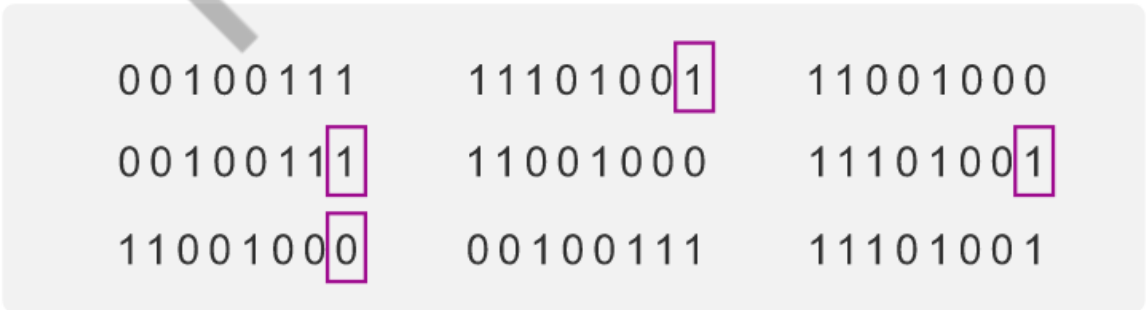

Figura 6.1 - Bits menos significativos de uma imagem
Fonte: Google Imagens (2020)

Com a introdução do valor binário 10000011 da mensagem em 9 pixels, iniciando do byte da esquerda superior, o resultado seria conforme a Figura “Bits menos significativos alterados”.

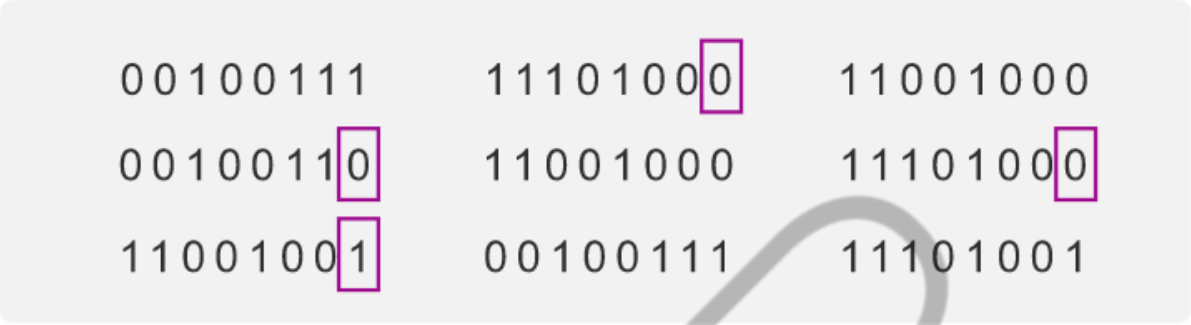

Figura 6.2 - Bits menos significativos alterados
Fonte: Google Imagens (2020)

b) Vicentini et. al. (2017) comenta que a filtragem e mascaramento modificam os bits mais significativos das imagens, ao contrário do LSB que utiliza os bits menos significativos e com fácil implementação. Por modificar os bits mais significativos, acaba tornando mais suscetível a detecção mas imperceptível a olho nu pelo ser humano.

c) Em algoritmos e transformações, as informações são inseridas em áreas mais robustas, que estão espalhadas pela imagem inteira, obtendo melhor resistência ao processar o sinal. As imagens no formato .jpeg utilizam a compressão em que há perda de dados (*Discrete Cosine Transform* – DTC), isso porque os valores cosseno são calculados imprecisamente, ocasionando introdução de arredondamento dos erros.

Conforme Vicentini et. al. (2017), a técnica baseada em algoritmos e transformações, tem como vantagem a compressão que é dos principais problemas encontrados no LSB. Nessa técnica, utiliza-se a transformada de Fourier discreta, transformada de cosseno discreta e transformada Z. Os dados ocultos são inseridos em áreas mais robustas, que estão alocadas em toda imagem, favorecendo resistência maior contra o processamento de sinal, porém, mesmo havendo técnicas sofisticadas, isso não quer dizer que implicará em melhor robustez para ataques de esteganálise.

d) A técnica de espalhamento de espectro difunde os dados ocultos na imagem cobertura, utilizando uma estego-chave para a seleção randômica dos

canais de frequência. A distribuição dos dados inseridos ocorre com a modulação destes por meio de pseudorruído e, após o processo, a energia é distribuída em uma larga faixa de frequência, que alcança apenas um nível muito inferior da força de inserção, garantindo a imperceptibilidade.

6.4 Métodos de detecção do uso da esteganografia

De acordo com Azevedo et. al. (2015), a Esteganálise – o estudo analítico de arquivos possivelmente esteganografados –, consiste na ideia de detectar uma mensagem oculta via esteganografia. Esse tipo de processo atua de duas formas: a primeira tem como objetivo identificar a presença de mensagens ocultas na imagem; a outra, extrair da imagem a mensagem oculta.

De acordo com Albuquerque (2007), os tipos de esteganálise são:

a) Ataques Aurais: retiram partes significativas do objeto de cobertura como um meio de facilitar a busca por ruídos adicionados via esteganografia;

b) Ataques Estruturais: visam procurar alterações no padrão do arquivo do objeto de cobertura;

c) Ataques Estatísticos: procuram encontrar padrões de comportamento do conteúdo do arquivo. Nos dias de hoje dificilmente são encontradas aplicações técnicas de ataques para mídias contínuas, ou seja, áudio e vídeo. O foco principal refere-se à esteganálise em imagens.

No estudo feito por Azevedo et. al. (2015), foi utilizada uma ferramenta de esteganografia que aceitava imagens do tipo “gif”, “jpeg”, “jpg” e “png”, e foram feitos testes com cada uma das extensões. Depois disso, por meio do terminal Linux, comparou-se o tamanho do arquivo original e o estaganografado. Como exemplo, foi embutida na abaixo a frase:

> Definições, assim como perguntas e metáforas, são instrumentos para fazer pensar. Sua autoridade reside inteiramente na sua utilidade, não na sua correção. Usamos definições a fim de delinear problema que desejamos investigar, ou favorecer interesses que queremos promover. Em outras palavras, inventamos definições e as descartamos na medida em que servem aos nossos propósitos (POSTMAN, 1980, p. 25).

Figura 6.3 - Figura original sem esteganografia
Fonte: Google Imagens (2020)

Após o processo, podem-se comparar as duas figuras, notando-se que não há nenhuma diferença, em nenhum dos cinco parâmetros analisados. Isso ocorre por causa do método LSB, que “esconde” a mensagem, possibilitando o seu envio de forma mais segura.

Figura 6.4 - Figura após ser submetida a esteganografia
Fonte: AZEVEDO et. al. (2015)

No experimento, foram esteganografadas dez figuras de cada uma das extensões (quatro tipos). As amostras possibilitaram obter um comparativo com os arquivos originais. Os critérios como formato da figura, qualidade e cor foram analisados visualmente. Já o tamanho dos pixels e do arquivo foi observado por meio do terminal Linux e foram consultadas as suas propriedades.

A “Figura após ser submetida a esteganografia” demonstra a imagem esteganografada, permitindo, assim, observar que, apesar de possuir uma mensagem em seu interior, não houve alterações visuais perceptíveis. Observou-se o mesmo comportamento em todas as extensões. Nenhuma das extensões apresentou qualquer tipo de alteração na figura que permitisse algum interceptador encontrar a mensagem embutida.

6.5 Ferramentas para esteganografia em imagens

Tomando como base a distribuição Kali Linux, utilizada em nossas aulas por ter seu foco em Segurança Cibernética, apresentaremos a ferramenta de terminal Steghide, utilizada para esteganografia de imagens.

De acordo com Azevedo et. al. (2015), o Steghide é um programa de esteganografia capaz de esconder dados em vários tipos de arquivos de áudio e de imagem. As frequências de som e de cor, respectivamente, não são alteradas tornando o arquivo resistente contra testes estatísticos de primeira ordem. O algoritmo de criptografia padrão é o Rijndael com uma chave de 128 bits de comprimento, no qual os “dados secretos” são compactados e criptografados. Em seguida, uma sequência de posições de pixels no arquivo que servirá de “esconderijo” é criada com base em um gerador de números aleatórios inicializado com a senha (os “dados secretos” serão incorporados nos pixels dessas posições). Posteriormente, um algoritmo de correspondência grafo-teórico encontra pares de posições tais que troquem seus valores. Isso tem o efeito de incorporar a parte correspondente dos “dados secretos”. Se o algoritmo não consegue encontrar mais pares, todas as trocas são efetivamente realizadas.

O Steghide usa o método LSB, ou seja, substitui o bit menos significativo dos pixels que formam as cores das imagens do tipo Bitmap (BMP) em imagens desse tipo, as cores nos pixels são formadas da seguinte maneira: imagens como “jpg” possuem blocos sucessivos de 8 bits, o que permite que se tenha 224 cores diferentes (uns 16 milhões de tonalidades), com 24 bits por pixel.

O método de esteganografia LSB vai substituir o bit menos significativo de cada uma das três cores que formam um pixel (RGB – Red [Vermelho], Green

[Verde] e Blue [Azul]), assim cada pixel aceita até três bits de informação; desse modo, cada imagem consegue armazenar até três vezes o número de pixels que possui, assim como demonstrado na Figura “Processo de esteganografia com Steghide”.

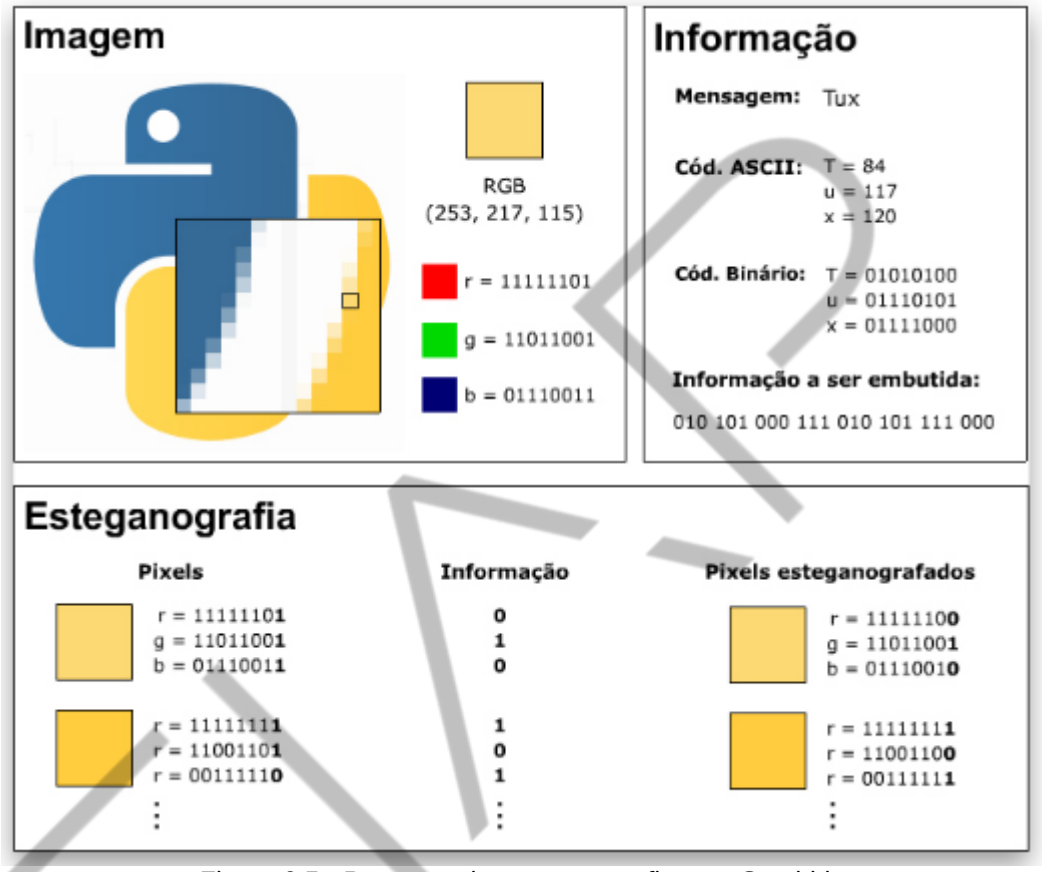

Figura 6.5 - Processo de esteganografia com Steghide
Fonte: Google Imagens (2020)

Outra ferramenta interessante, apesar de não vir por padrão no Kali Linux é o Stegsolv. Escrito em Java, o Stegsolv foi desenvolvido para ataques aurais em imagens, nas quais ele aplica diversos filtros, como, por exemplo, inversão de cores (XOR), para que o analista consiga identificar visualmente conteúdos escondidos em imagens por meio da esteganografia.

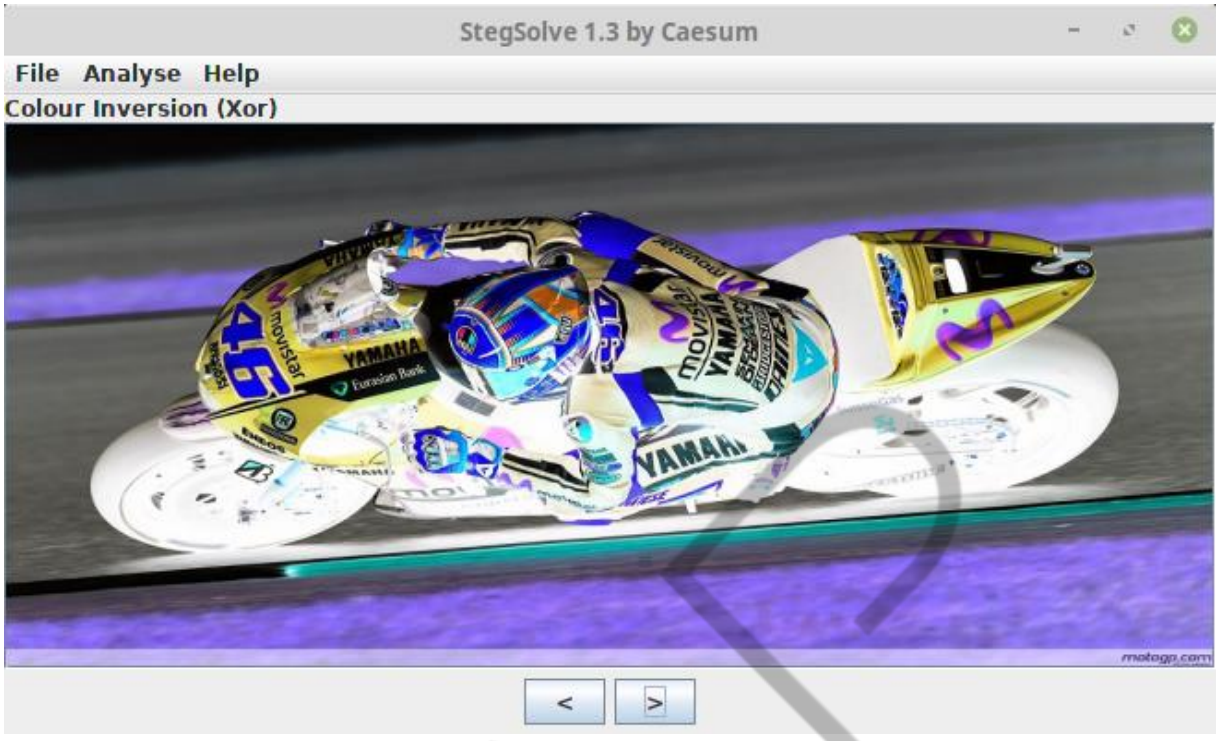

Figura 6.6 - Stegsolv com filtro de inversão de cores XOR
Fonte: Elaborado pelo autor (2020)

Ferramentas de esteganografia, a exemplo do Steghide, além de embutirem conteúdos em imagens, conseguem protegê-los da decifragem com senhas. Logo, em uma estegoanálise na qual se identifique a existência de conteúdo esteganografado em imagem, porém não se consiga extrair em razão da necessidade de senha, existem ferramentas como o StegCrack, que conseguem automatizar um ataque de dicionário (*password guessing*) na imagem esteganografada.

Quanto à detecção da esteganografia por meio de ataques estruturais, podemos citar ferramentas como o StegDetec, que, aplicado à imagem analisada, traz informações quanto ao possível conteúdo esteganografado. Porém, no caso da esteganografia ter sido feita pelo Steghide, uma forma simples de identificar é analisando a imagem com o comando strings (presente no Kali Linux), tendo em vista que o steghide deixa um padrão de assinatura na imagem esteganografada, conforme a Figura “Imagem JPG “stringada” sem assinatura de uso do Steghide” e a Figura “Imagem JPG “stringada” com assinatura de uso do Steghide”.

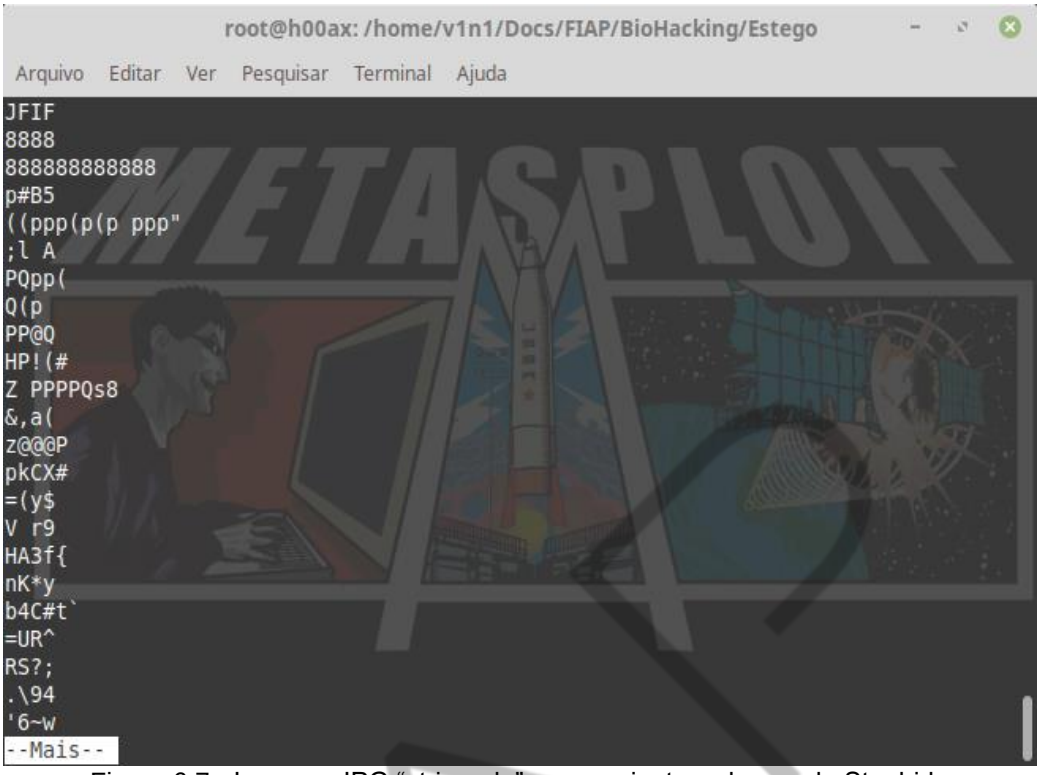

Figura 6.7 - Imagem JPG “stringada” sem assinatura de uso do Steghide
Fonte: Elaborado pelo autor (2020)

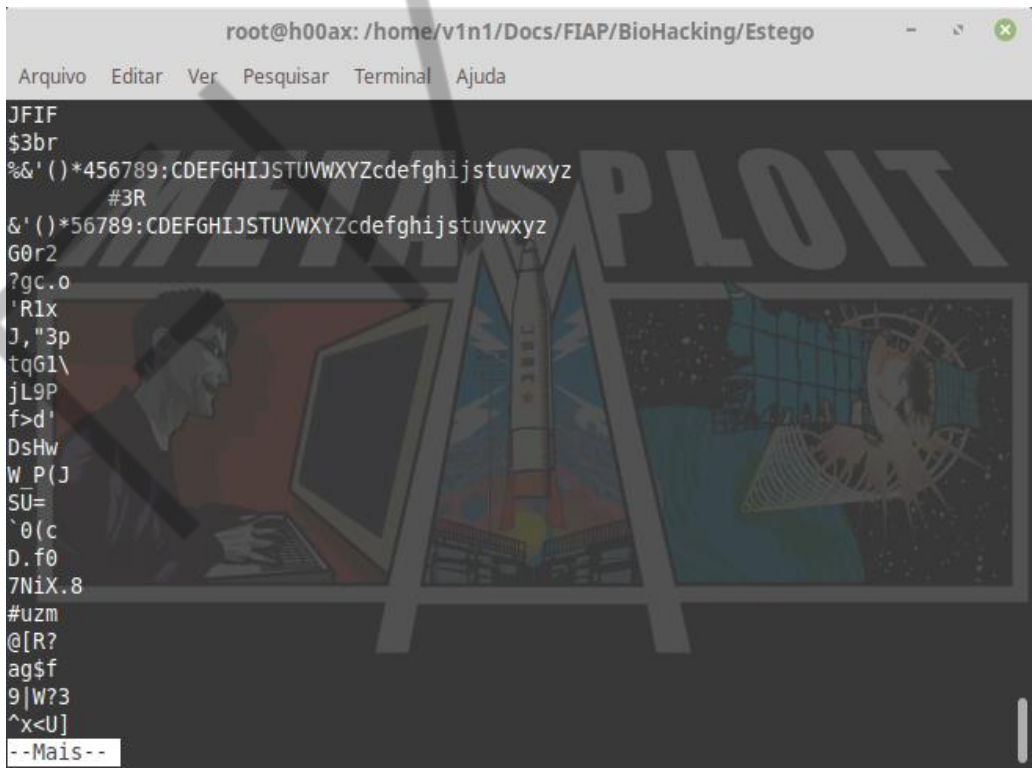

Figura 6.8 - Imagem JPG “stringada” com assinatura de uso do Steghide
Fonte: Elaborado pelo autor (2020)

6.6 Lab

Neste LAB, vamos esteganografar um conteúdo em uma imagem, utilizando o Kali Linux e a ferramenta Steghide.

Baixe neste link (http://veloxtv.com.br/wp-content/uploads/2015/08/v-rossi.jpg) a imagem modelo que usaremos para sua máquina virtual do Kali Linux e execute os procedimentos a seguir.

a) Preparação do conteúdo que será embutido na imagem:

Abra o editor de textos nano através do terminal do seu Kali e crie o arquivo “fiap.txt” com o seguinte conteúdo:

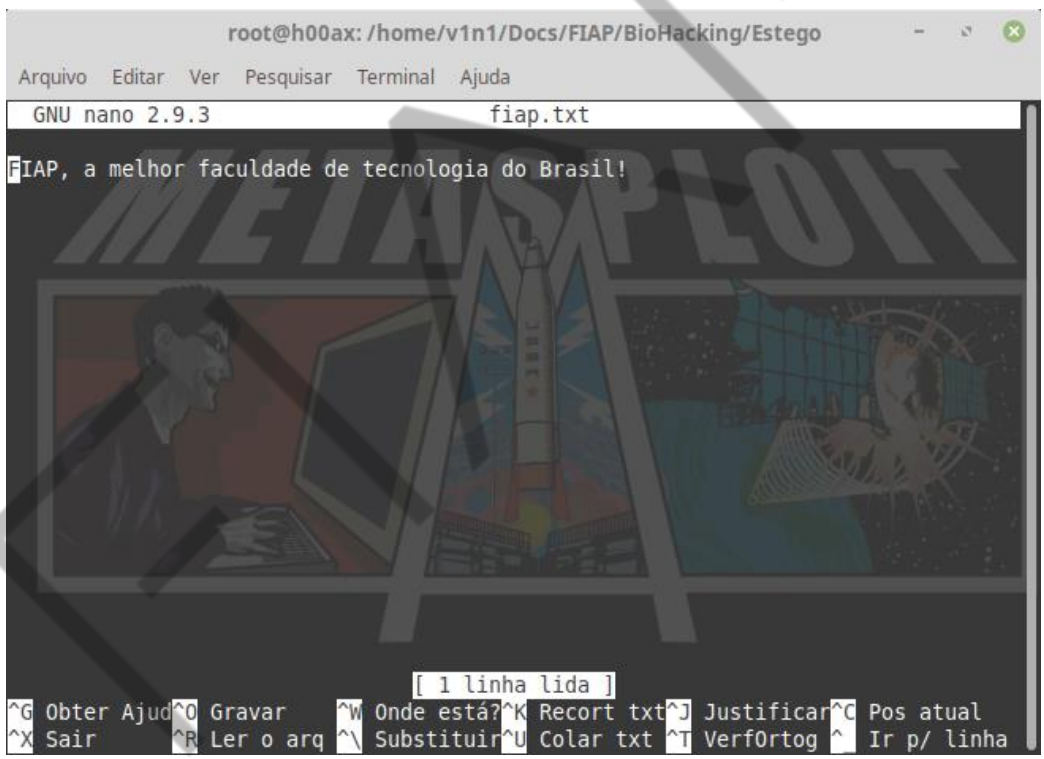

Figura 6.9 - Criação de conteúdo com o editor nano
Fonte: Elaborado pelo autor (2020)

Pressione Ctrl+O para salvar e depois Ctrl+X para sair do arquivo.

b) Esteganografando a imagem:

Utilizando o Steghide, embutiremos o arquivo “fiap.txt” na nossa imagem modelo conforme a sintaxe abaixo (escolha uma senha de sua preferência):

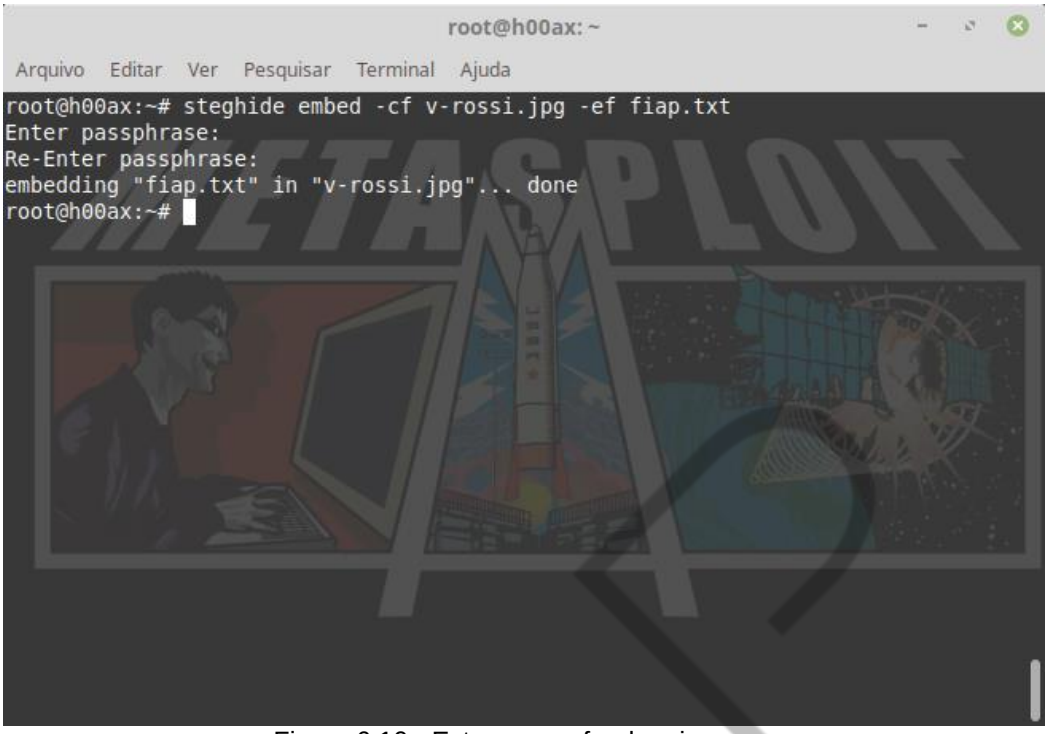

Figura 6.10 - Esteganografando a imagem
Fonte: Elaborado pelo autor (2020)

c) Conferindo a assinatura do Steghide:

Usando o strings, analisaremos a imagem modelo para identificar o padrão de assinatura do steghide, com a sintaxe abaixo (para sair do prompt do strings basta pressionar a tecla “q”):

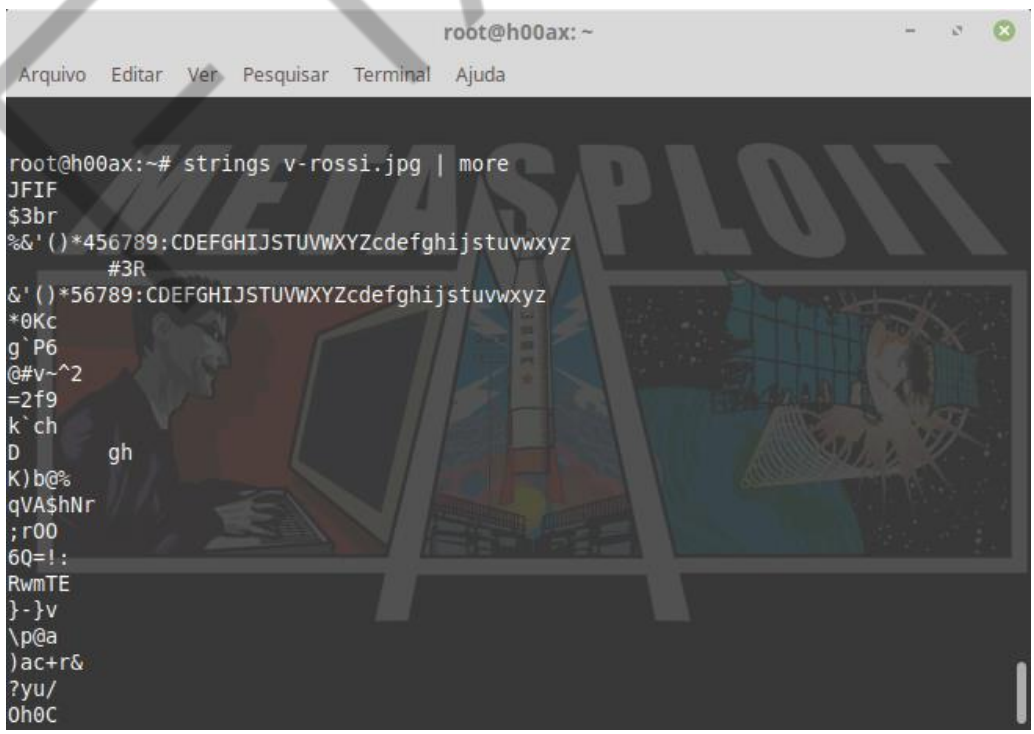

Figura 6.11 - Analisando a imagem
Fonte: Elaborado pelo autor (2020)

d) Revelando o conteúdo esteganografado da imagem:

Utilizaremos a sintaxe abaixo do Steghide para exibir o conteúdo esteganografado da imagem. Antes, para que o arquivo de saída não se confunda com o arquivo “fiap.txt” que está no diretório corrente, crie um subdiretório e mova a imagem modelo para lá antes de utilizar o Steghide para remover a esteganografia, desta forma:

```
mkdir estego
mv v-rossi.jpg estego/
cd estego
```

Agora, sim, utilize o Steghide para revelar o conteúdo da imagem modelo.

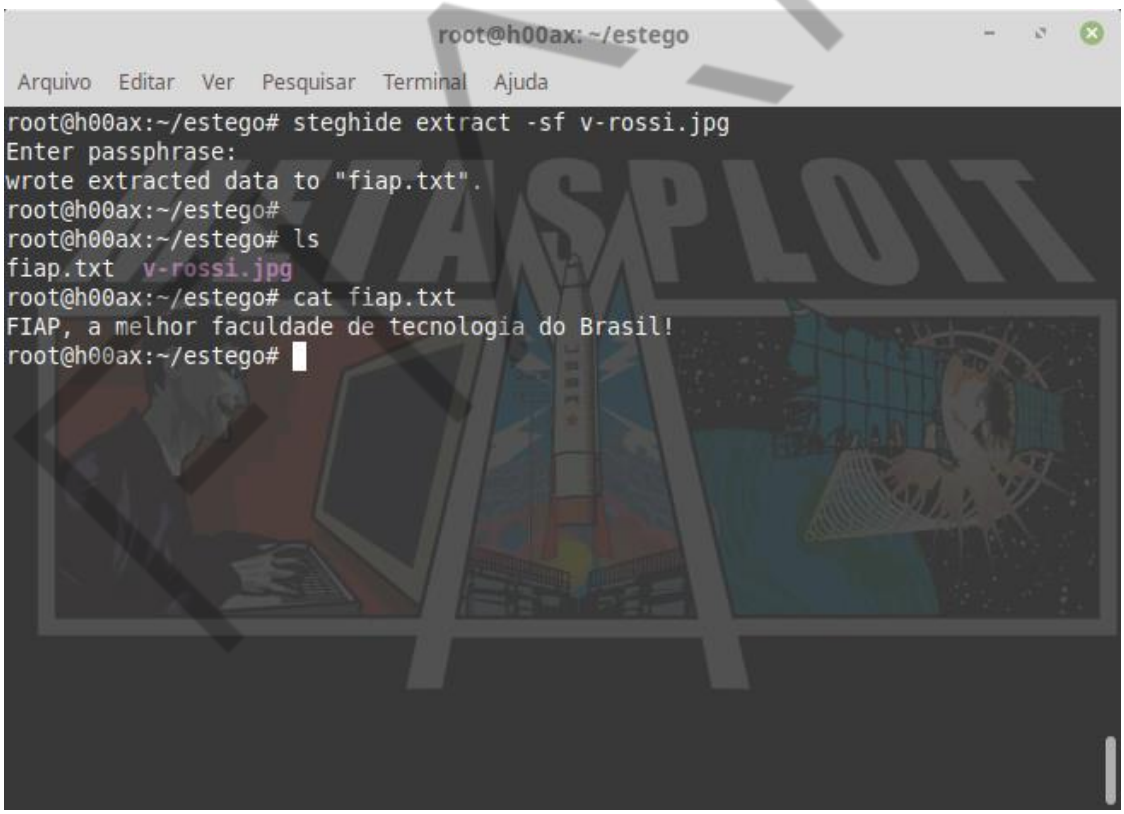

Figura 6.12 - Revelando o conteúdo da imagem esteganografada
Fonte: Elaborado pelo autor (2020)

REFERÊNCIAS

AZEVEDO, Eduardo, FAVERI, João Gabriel, NUNES, Sergio Eduardo. **Esteganografia**. 2015. Disponível em: <http://pgsskroton.com.br/seer/index.php/rcext/article/view/3401>. Acesso em: 16 jun. 2020.

VICENTINI, Fernanda R. S., OLIVEIRA, Henrique C., GODOY, Mario A., MARTINS, Henrique P. **Técnicas de Segurança**: Aplicação de Esteganografia em Imagens. 2017. Disponível em: <http://www.fatecbauru.edu.br/ojs/index.php/CET/article/view/283>. Acesso em: 16 jun. 2020.