CRIMES CIBERNÉTICOS: UM COMPARATIVO DE TÉCNICAS DE ESTEGANOGRAFIA UTILIZADAS PARA OCULTAÇÕES DE INFORMAÇÕES.

Camila Pellizon Floret.[1] Elvio Gilberto da Silva. Henrique Pachioni Martins. Patrick Pedreira Silva.

RESUMO

As redes de computadores interligadas do mundo inteiro facilitam a troca de dados e informações em poucos milissegundos. A segurança da informação está relacionada com as variedades de ameaças que os dados são expostos nas redes. A perícia forense computacional tem como objetivo localizar informações registradas ou transmitidas em forma binária, nas quais podem ser utilizadas como prova em processos penais, civis e administrativas. Para que as evidências sejam válidas é necessária à realização de um processo de investigação. Existem diversos tipos de técnicas anti-forenses, nas quais vale ressaltar a criptografia e esteganografia. A criptografia permite a alteração da informação a torná-la compreensível a terceiros por meio da técnica de esteganografia, que é a escrita cifrada de textos com caracteres convencionais, sendo letras, números ou símbolos, nas quais podem ser camufladas em áudios, imagens e vídeos. Os crimes informáticos são caracterizados pela elevada incidência de ações ilícitas penais que apresentam como meio desta prática um dispositivo eletrônico. Os principais objetivos deste trabalho incidem em efetuar uma análise bibliográfica sobre os conceitos de esteganografia, pesquisar os softwares de perícia forense digital que possibilitam na verificação dos arquivos, comparar e relatar as diferenças dos arquivos originais dos modificados, identificando as vantagens e desvantagens da utilização das técnicas. A metodologia utilizada consiste em analisar as imagens em diversas extensões, como JPEG, PNG e BMP, e dimensões, de 256, 512, e 1024 pixels, através dos softwares Backtrack or Kali Linux, Computer Aided Ambiente Investigativo (Caine), Helix3, e Forense Digital Toolkit (FDTK). Os testes foram feitos no Binwalk do Backtrack ou Kali Linux, Okteta do Caine, Outguess e Hexdump do FDTK, e Bless Hex Editor do Helix3. Posteriormente, após a inserção da mensagem nas imagens, foi comparado com os resultados obtidos, o alvo é encontrar os dados que não correspondem ao arquivo original, acessando os valores hexadecimais das imagens esteganografada, de acordo com cada ferramenta.

Palavras-chave: Segurança da informação. Perícia forense computacional. Esteganografia.

1 INTRODUÇÃO

[1]Graduanda em Ciência da Computação pela Universidade do Sagrado Coração (USC). cacafloret@gmail.com

A segurança da informação tem como principal objetivo proteger as informações de uma organização ou indivíduo. Com o aumento do uso das redes e aplicações interligadas, o sistema ou máquina podem estar comprometidos e tudo que está ao redor também.

Uma das técnicas universais é a criptografia na qual é a arte do texto escrito ou dado em um código secreto. Trata-se de dados em um simples formato ilegível chamado de texto cifrado. (COUNCIL, 2009). A esteganografia é o ramo particular da criptologia que consiste em fazer com que uma forma escrita seja camuflada com o propósito de encapotar sua verdadeira essência. (PINOCHET, 2014).

Por se referir a um conteúdo muito abrangente é fundamental estar diante das investigações e pesquisas de novos meios tecnológicos para atividades criminosas. Com base nesse contexto, o presente trabalho tem como intuito colaborar com atividades futuras envolvendo os comparativos de ferramentas de esteganografia, que tem por principio manter a integridade e segurança da informação, principalmente contribuir com interessados na área de segurança, como por exemplo, peritos forenses, ou até mesmo estudantes das áreas de tecnologia da informação.

1.1 OBJETIVOS

Nos próximos tópicos foram apresentados o objetivo geral e os objetivos específicos.

1.1.1 Objetivos gerais

Explorar técnicas de esteganografia digital por meio de comparativo de ferramentas open-source, a fim de demonstrar as vantagens e desvantagens da utilização das de cada uma das técnicas estudadas.

1.1.2 Objetivos específicos

a) efetuar uma análise bibliográfica sobre os conceitos de esteganografia;

b) pesquisar e selecionar sobre os softwares de perícia forense digital que possibilitem na verificação dos arquivos de tamanhos e extensões específicas;
c) comparar e relatar as diferenças encontradas dos arquivos originais dos modificados;
d) identificar as vantagens e desvantagens da utilização das ferramentas técnicas.

2 REVISÃO DE LITERATURA

Abaixo serão discutidos os assuntos sobre segurança da informação, perícia forense, técnicas de ataque e as tecnologias utilizadas, e crimes informáticos.

2.1 SEGURANÇA DA INFORMAÇÃO

A importância da segurança da informação vem a proteger as infraestruturas críticas dos negócios, envolvendo setores públicos e privados. Muitos sistemas não foram projetados para serem seguros, porém a preservação das informações pode ser alcançada por meio técnicos limitados, e devem ser apoiadas por uma gestão e procedimentos apropriados.

2.1.1 Política de segurança

A política de segurança da informação tem como objetivo proporcionar um apoio, e uma orientação sendo analisada de tempos em tempos, verificando-se de acordo com os requisitos as possíveis mudanças e as regulamentações relevantes.

Conforme Marciano (2006), os ambientes organizacionais estão sujeitos a diversos eventos e potencialidades, divididos em três categorias: ameaças, vulnerabilidade e incidentes, compondo e caracterizando os riscos à segurança.

2.1.2 Arquitetura de segurança

Para medir as necessidades de segurança de uma organização, avaliar e escolher inúmeros produtos e políticas de segurança, os responsáveis precisam de

algum meio sistemático de delimitar as condições de segurança e caracterizar as técnicas para satisfazer os requisitos. De acordo com Stallings (2007), o foco desta estrutura são os ataques ativos e passivos, mecanismos e serviços.

2.1.3 Criptografia

A criptografia é a arte de codificação que permite a modificação reversível da informação de forma a torná-la compreensível a terceiros. É utilizada em determinados algoritmos numa chave secreta, para que a partir do conjunto de dados não criptografados possa produzir uma sequência de dados criptografados.

De acordo com Oliveira (2012), há dois tipos de criptografia que são criptografia simétrica, que são protocolos baseados em algoritmos que requerem duas chaves uma delas são a privada e a outra pública, e a criptografia assimétrica que é a chave é o elemento que dá acesso à mensagem oculta trocada entre duas partes, ou seja, é igual para ambas e deve permanecer em segredo.

2.2 SEGURANÇA EM SISTEMAS COMPUTACIONAIS

De acordo com Almeida et al. (2014), há três princípios que são confidencialidade, integridade e disponibilidade. A explicação resumida é que somente pessoas autorizadas devem ter acesso à informação, aos quais não deverá ter alterações, aquelas que foram autorizadas serão salvas pelo proprietário e a informação deverá estar sempre disponível, se um ou mais desses princípios forem desobedecidos, temos um incidente de segurança em sistemas computacionais.

2.3 PERÍCIA FORENSE COMPUTACIONAL

A perícia forense computacional é um ramo da ciência forense que se concentra na lei de processo penal e evidências como aplicadas a computadores e dispositivos relacionados, não se limita apenas em computadores, mas também inclui telefones móveis, PDA (assistente digital pessoal) e redes. Segundo Eleutério e Machado (2011), computação forense é informação armazenada ou transmitida de forma binária, que podem ser usados como prova em processos penais, civis e

administrativas. Esses dados podem ser encontrados a partir de dispositivos eletrônicos.

Os crimes comentidos com o uso de equipamentos computacionais, segundo Gonçalves et al. (2012), podem ser especificados de duas modalidades, que são o computador utilizado como ferramenta de apoio à prática de delito e computador utilizado como meio para a realização do delito. De acordo com Romeiro (2002), os crimes de informática devem ser classificados quanto ao seu objetivo material, que no caso são crimes de informática comum, crimes informática misto e crimes informática puro.

Os locais de crime envolvendo os equipamentos computacionais são onde as supostas infrações penais ocorreram. Podemos encontrar evidências muito úteis à investigação, com o propósito de esclarecer a autoria (quem), dinâmica (como) e materialidade do delito (o que aconteceu). (ELEUTÉRIO; MACHADO, 2011).

Conforme Eleutério e Machado (2011), os peritos e suas equipes devem realizar um reconhecimento na área do crime, identificando os equipamentos computacionais. Os profissionais capacitados devem ter o conhecimento em equipamentos e técnicas forenses para verificar o conteúdo armazenado nos dispositivos, permitindo com que nenhuma informação seja modificada, garantindo a preservação das evidências digitais.

De acordo com Fagundes et al. (2007) as evidências são peças fundamentais para uma investigação. Para que sejam válidas é necessária à realização de um processo de investigação de maneira curiosa e sistemática.

2.4 TÉCNICAS DE ATAQUES

Os ataques são métodos de remoção, ocultação e subversão de evidências com o objetivo de suavizar os resultados de análises forenses computacionais, a fim de dificultar o trabalho dos peritos. Existem vários tipos de técnicas anti-forenses, nas quais destacamos abaixo.

2.4.1 Destruição de dados

A ferramenta conhecida como wiping tools são utilizadas para dificultar ou impedir a recuperação dos dados, ou seja,

> destruindo os dados que ficam armazenados no HD. Além desta destruição lógica, em alguns casos, os criminosos podem danificar fisicamente as mídias dificultando e até impossibilitando a recuperação dos dados. (FAGUNDES, 2007; KONRATH, 2007; LUDWIG, 2007; NEUKAMP, 2007; PEREIRA, 2007).

2.4.2 Limpeza de registros

Segundo Fagundes et al. (2007), os registros são bancos de dados que armazenam as configurações e opções de todos os hardwares. Os softwares de limpeza de registros são capazes de zerar e sobrescrever arquivos de dados, qualquer tipo de recuperação se torna impraticável ou até impossível de ser realizada.

2.4.3 Modificação de dados

Conforme Fagundes et al. (2007), há dois tipos comuns para realizar a modificação dos dados que são alterar a extensão dos arquivos e modificar o conteúdo do cabeçalho dos arquivos.

2.4.4 Ocultação de dados

Segundo Albuquerque et al. (2007), os dados podem ser escondidos de duas formas, digital watermarking e esteganografia. Apesar de aparecerem quase sempre em conjunto com a esteganografia, o sistema digital watermarking não pertence ao mesmo ramo da esteganografia.

2.4.5 Digital watermarking

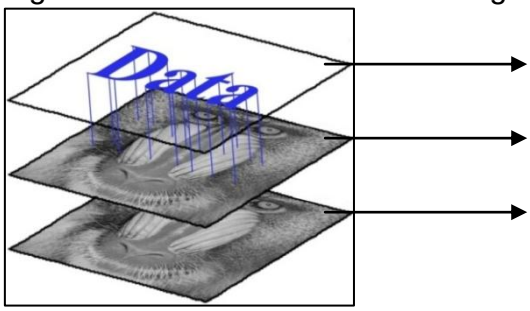
Este método de técnica digital é conhecido como marca d’água em que se refere a um sinal portador de informações, visivelmente imperceptível introduzido em uma imagem digital. A imagem que contém a marca é considerada como imagem hospedeira ou marcada.

2.4.6 Esteganografia

Esteganografia é a arte de camuflar informações em que não sejam percebidas. Segundo Alencar (2015) é a escrita cifrada de textos com caracteres convencionais, que podem ser letras, números ou símbolos.

O resumo do processo de esteganografia baseia-se na mensagem secreta enviada ao recipiente, na qual será camuflada em vários tipos de arquivos. O stego-object é a união dos dois componentes citados anteriormente. Por fim, o resultado do método que foi utilizado para controlar esse processo de esconder e recuperar dados secretos. A Figura 1 mostra como os dados são embutidos na imagem.

Figura 1 – Funcionamento da esteganografia



I – Dados a serem embutidos.

II – Dados são embutidos na imagem com uso de uma chave (stego-key).

III – O stego-object é criado contendo a informação escondida.

Fonte: Li (2015).
Nota: Adaptada pela autora.

Os dados embutidos são inseridos em algum arquivo de maneira sigilosa. A mensagem coberta é o arquivo que servirá de esconderijo para o dado que será embutido. A chave (stego-key) poderá ser usada ao inserir dados na mensagem coberta. O resultado final (stego-object) da mensagem coberta possuirá as informações que foram inseridas secretamente.

2.4.6.1 Esteganografia em áudios, imagens e vídeos

As técnicas de esteganografia em áudios exploram a vulnerabilidade do sistema auditivo humano podendo captar até um bilhão de potências diferentes e até mil frequências de sinais distintas. A tendência é que os sons mais altos prevalecem do que os sons mais baixos, além que existem algumas distorções dos ambientes que simplesmente são ignoradas pelo ouvido.

Existem diversas técnicas indicadas a seguir que manuseiam com imagens, que são a técnica de inserção do least significant bit, as técnicas de filtragem e mascaramento, e as técnicas de algoritmos e transformações. Segundo Carvalho

(2005), a esteganografia de imagem é similar à esteganografia de vídeos, exceto pelo fato das informações estarem ocultas em diversões quadros ou frames dos arquivos, criando uma grande complexidade nas buscas destes dados.

2.5 CRIMES INFORMÁTICOS

De acordo com Daoun e Lima (1999) há várias expressões utilizadas de forma equivocada como crimes de informática, crimes tecnológicos, crimes cibernéticos, crimes virtuais etc. No entanto, o termo crimes informáticos traduz, de forma abrangente, os crimes praticados contra ou pelo uso informatizado englobando-se aqueles cometidos na rede mundial de computadores.

3 METODOLOGIA

Na primeira foi elaborada o referencial teórico, na qual foram realizadas pesquisas em livros, artigos científicos e outros trabalhos focados na área de segurança da informação, perícia forense computacional e os softwares que serão utilizados no decorrer do trabalho. Na segunda etapa foi elaborada a parte prática utilizando os softwares de esteganografia, para a qual foram escolhidos o Backtrack ou Kali Linux, Caine, Helix e FDTK.

A aplicação das análises de esteganografia será realizada em um notebook particular do fabricante Acer, modelo Aspire 5750, plataforma Windows 7, sistema operacional de 64 bits, processador Intel Core i3-2330 CPU @ 2.20 GHz e 4 GB de memória RAM. Os softwares escolhidos são funcionais em apenas plataforma Linux, no caso, será feito a instalação de uma máquina virtual Oracle VM VirtualBox versão 5.1.4, lançada em 16 de agosto de 2016, que foi escolhida pela compatibilidade com qualquer sistema operacional.

O Backtrack ou Kali Linux versão 1.1.0 foi selecionado por ter características de interface gráfica de fácil manuseio, e que inclui um scanner de portas, um analisador de pacotes, um cracker de senhas, e uma suíte de software para redes sem fio de teste de penetração, e possui uma flexibilidade na distribuição.

O Caine versão 7.0 foi escolhido por ser uma interface gráfica de fácil manuseio, de inicialização rápida, e bloqueia todos os dispositivos de bloco

frequentemente utilizados em dispositivos de comunicação paralela como discos rígidos e drives de CDs, em modo de somente leitura.

O FDTK versão 3.0 foi selecionado por ter suas vantagens de uma interface gráfica de fácil manuseio, baseada em idioma português, possui etapas como coleta, exame, análise de dados e toolkits.

O Helix3 versão ISO2008R1 foi escolhido por ter suas vantagens de não inicializar o disco rígido, e possui um kit básico que inclui antivírus, análises de redes, recuperadores de senhas, examinador de arquivos binários, etc.

Após a instalação dos softwares open-source serão executadas as imagens de extensões BMP, que podem suportar milhões de cores e conservar os detalhes, o JPEG, que tem tamanho pequeno quando comparado a outros formatos, facilitando o seu armazenamento e a sua distribuição, e por fim, o PNG, que suporta milhões de cores mantendo a qualidade das imagens, e de dimensões, de 256, 512, e 1024 pixels, que são as mais utilizadas pelos usuários de informática.

A escolha das imagens coloridas levará à identificação da modificação do pixel, analisando o que cada ferramenta suporta. Os testes foram feitos no Binwalk do Backtrack ou Kali Linux, Okteta do Caine, Outguess e Hexdump do FDTK, e Bless Hex Editor do Helix3.

Posteriormente, as imagens inseridas foram comparadas aos resultados obtidos, acessando os valores hexadecimais do arquivo original e do arquivo modificado. O alvo foi encontrar os valores que não correspondem ao arquivo original.

4 RESULTADOS FINAIS

Com a atualização na plataforma Windows 7 Home Basic para Windows 10 Home e do Virtual Oracle versão 5.0.20 para 5.1.4 disponível no dia 16 de agosto de 2016, foram efetuados os downloads dos softwares Backtrack ou Kali Linux versão 2016.1, Caine versão 7.0, FDTK versão 3.0, e Helix versão ISO2008R1.

O arquivo com o nome de “Mensagem” foi elaborado em formato TXT, tamanho 1 KB, na qual inseriu a seguinte frase sem acentos, “Uma perícia bem feita, é capaz de fazer dos vestígios deixados na cena do crime, a única testemunha capaz de expressar a verdade absoluta e, portanto, a justiça que sempre se busca”.

No Backtrack ou Kali Linux foi usado o Binwalk versão 2.1.1, pois é uma ferramenta de fácil manuseio e as características mais importantes para o desenvolvimento do trabalho são a localização e extração dos arquivos binários.

O Caine apresenta uma ferramenta chamada Okteta versão 0.13.3 foi empregada por ser um editor de dados de arquivos e foi usada para comparar as imagens em diversos tamanhos e extensões. Podendo ser codificada binário, decimal, octal e hexadecimal.

No FDTK, foi utilizado o Hexdump é um comando que obtém a entrada a partir de um arquivo ou de uma entrada padrão, fornecendo muitas opções para extrair e depurar o conteúdo do arquivo escrito por qualquer programa de aplicação.

No Helix3, a ferramenta Bless Hex Editor, é um editor binário que permite editar arquivos como sequência de byte.

5 CONSIDERAÇÕES FINAIS

Neste trabalho foram apresentados os conceitos de segurança da informação, perícia forense computacional, técnicas de ataque, com foco em esteganografia, e crimes informáticos. Além disso, na parte prática foram apresentados quatros softwares de esteganografia que utilizam diferentes ferramentas para ocultação e comparação de dados das imagens digitais.

As técnicas de esteganografia têm seu uso legal e ilegal. Como uso legal no presente e no futuro, esteganografia tem sido usada e será cada vez mais utilizada na proteção de direitos, principalmente quando se considera as novas formas de comercialização utilizando a mídia digital.

As escolhas dos softwares destacaram por serem ferramentas open-source, de plataforma Linux, e por diferenciar o método como foi obtido no resultado.

O Backtrack ou Kali Linux fornece uma interface mais complexa, uma vez que é necessário compreender cada linha de comando da ferramenta Binwalk, e consequentemente, qual a melhor opção para empregar. Para aqueles que não conhecem a língua inglesa, esta ferramenta não é considerada com boa opção de uso.

O software Caine é de interface amigável ao usuário. A ferramenta Okteta é um editor simples para os dados brutos dos arquivos. Para aqueles que desejam

uma comparação rápida e eficiente, esta ferramenta é considerada como uma ótima opção de escolha.

O FDTK é fácil de manusear, visto que é necessário abranger cada linha de comando das ferramentas Hexdump, que obtém a entrada a partir de um arquivo ou de uma entrada padrão, fornecendo muitas opções para extrair e depurar, e o Outguess, que realiza a análise da imagem e utiliza a técnica de substituição dos bits menos significativos para ocultar as mensagens inseridas na imagem original. Para aqueles que não têm conhecimento da língua inglesa, esta ferramenta não é apropriada para o seu uso.

O software Helix3 fornece uma interface simples na execução. A ferramenta Bless Hex Editor, é um editor binário que permite editar arquivos como sequência de byte. Para aqueles que desejam uma comparação ligeira e eficiente, esta ferramenta é considerada como uma ótima escolha.

Por fim, todos os softwares apresentaram vantagens e desvantagens, no entanto tiveram um desempenho excelente na execução e obtiveram-se os resultados positivos, ou seja, mensagem oculta no arquivo modificado foi localizada. Neste trabalho as comparações forma feitas em três softwares distintitos, o Backtrack ou Kali Linux, Caine, e Helix3, e um software igual, o FDTK, sendo todas utilizadas em plataforma Linux.

CYBER CRIMES: A STEGANOGRAPHY COMPARATIVE TECHNIQUES USED FOR INFORMATION OCCULTATIONS. Camila Pellizon Floret. Elvio Gilberto da Silva. Henrique Pachioni Martins. Patrick Pedreira Silva.

ABSTRACT

Interconnected computer networks around the world make it easy to exchange data and information in just a few milliseconds. Information security is related to the varieties of threats that the data is exposed on the networks. Computer forensics aims to locate information recorded or transmitted in binary form, in which it can be used as evidence in criminal, civil and administrative proceedings. For the evidence to be valid, it is necessary to carry out a process of investigation. There are several types of anti-forensic techniques, in which it is worth emphasizing the cryptography and steganography. Encryption allows the change of the information to make it

comprehensible to third parties through the technique of steganography, which is the encrypted writing of texts with conventional characters, being letters, numbers or symbols, in which they can be camouflaged in audios, images and videos . Computer crimes are characterized by the high incidence of illegal criminal actions that present as a means of this practice an electronic device. The main objectives of this work are to carry out a bibliographical analysis on the concepts of steganography, to search for digital forensics software that allows the verification of the files, to compare and to report the differences of the original files of the modified ones, identifying the advantages and disadvantages of using the Techniques. The methodology used consists of analyzing the images in various extensions, such as JPEG, PNG and BMP, and dimensions of 256, 512, and 1024 pixels, through Backtrack or Kali Linux, Computer Aided Investigative Environment (Caine), Helix3, and Forensic Digital Toolkit (FDTK). The tests were done on Backtrack's Binwalk or Kali Linux, Caine's Okteta, Outguess and Hexdump from FDTK, and Helix's Bless Hex Editor3. Subsequently, after the insertion of the message in the images, was compared with the results obtained, the target is to find the data that do not correspond to the original file, accessing the hexadecimal values of the steganogramed images, according to each tool.

Keywords: Information security. Computer forensics. Steganography.

REFERÊNCIAS

ALBUQUERQUE, Célio Vinicius Neves; JULIO, Eduardo Pagani; BRAZIL, Wagner Gaspar. **Esteganografia e suas aplicações.** 2007. 49 f. Trabalho de Conclusão de Curso (Doutorado em Computação) - Universidade Federal Fluminense, Niterói, 2007.

ALENCAR, Marcelo Sampaio. **Informação, codificação e segurança de redes.** Rio de Janeiro: Elsevier, 2015. Disponível em: <https://books.google.com.br/books?id=jpbpCgAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em: 29 abr. 2016.

ALMEIDA, Daniela; AMARAL, Érico; FREITAS, Mariana Pompeo; JACOBSEN, Wilson; PINHO, Leonardo; ROTONDO, Gustavo. **Da computação forense a técnica de esteganografia. Um ensaio sobre a ocultação de informações em sistemas computacionais.** 2015. 10 f. Trabalho de Conclusão de Curso

(Graduação em Engenharia da Computação) – Universidade Federal do Pampa, Bagé, 2015.

COUNCIL, E-C. **Computer forensics: investigating network intrusions and cybercrime.** Clifton Park: Course Technology, 2009. Disponível em: <https://books.google.com.br/books?id=FfoFAAAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false>. Acesso em: 30 abr. 2016.

DAOUN, Alexandre Jean; TRUZZI DE LIMA, Gisele. Crimes informáticos: O direito penal na era da informação. In: IV Conferência Internacional de Perícias em Crimes Informáticos, 1., 2007, Guarujá. **Resumos...** Guarujá: Instituto Brasileiro Design Interiores, 2006. p. 11.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a computação forense.** 1 ed. São Paulo: Novatec, 2011.

FAGUNDES, Leonardo Lemes; KONRATH, Marlom; LUDWIG, Glauco; NEUKAMP, Paulo; PEREIRA, Evandro Della Vecchia. **Forense computacional: fundamentos, tecnologias e desafios atuais.** 2007. 51 f. Trabalho de Conclusão de Curso (Mestrado em Ciência da Computação) – Universidade do Vale do Rio dos Sinos, São Leopoldo, 2007.

FIORI DE CARVALHO, Diego. **Exploração tecnológica para esteganografia em vídeos digitais.** 2005. 211 f. Teste (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2005.

GONÇALVES, Louis Augusto. **Um estudo sobre a transformada rápida de Fourier e seu uso em processamento de imagens.** 2004. 57 f. Dissertação (Mestrado em Matemática Aplicada) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2004.

MARCIANO, João Luiz Pereira. **Segurança da informação – Uma abordagem social.** 2006. 211 f. Teste (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

OLIVEIRA, Ronielton Rezende. **Criptografia tradicional simétrica de chave privada e criptografia assimétrica de chave pública: análise das vantagens e desvantagens.** 2006. 20 f. Trabalho de Conclusão de Curso (Pós-Graduação em Criptografia e Segurança em Redes) – Universidade Federal Fluminense, Niterói, 2006.

PINOCHET, Luis Hernan Contreras. **Tecnologia da informação e comunicação.** Rio de Janeiro: Elsevier, 2014. Disponível em: <https://books.google.com.br/books?id=plgaBQAAQBAJ&pg=PT233&dq=esteganografia&hl=pt-BR&sa=X&ved=0ahUKEwjC7oy-

9IzNAhXCSSYKHRkqCUgQ6AEIHDAA#v=onepage&q=esteganografia&f=false>. Acesso em: 10 abr. 2016.

ROMEIRO, Leandro Kawa. **Crimes de informática.** 2002. 43 f. Trabalho de Conclusão de Curso (Graduação em Direito) – Faculdade de Ciências Jurídicas, Universidade Tuiuti do Paraná, Curitiba, 2002.

STALLINGS, William. **Criptografia e segurança de redes – Princípios e práticas.** 4 ed. São Paulo: Prentice Hall Brasil, 2008.