

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

Camila Pellizon Floret¹. Henrique Pachioni Martins².

¹Centro de Ciências Exatas e Sociais Aplicadas – Universidade do Sagrado Coração – cacafloret@gmail.com

²Centro de Ciências Exatas e Sociais Aplicadas – Universidade do Sagrado Coração – henrique.martins@usc.br

Tipo de pesquisa: TCC

Agência de fomento: Não há

Área do conhecimento: Exatas – Ciência da Computação

As redes de computadores interligadas do mundo inteiro facilitam a troca de dados e informações. A inovação tecnológica ocasiona inúmeros benefícios para as pessoas e a comunidade em geral, porém essa facilidade possibilita algumas práticas ilegais e criminosas. A segurança da informação está relacionada com as variedades de ameaças que os dados são expostos nas redes, os pilares cruciais desta segurança são a disponibilidade, integridade e confidencialidade. 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. De modo que as evidências sejam válidas é necessária à realização de um processo de investigação aos quais contém as fases de coleta, exame, análise e resultado. Existem diversos tipos de técnicas anti-forenses, nas quais vale ressaltar a destruição de dados, limpeza de registros, modificação de dados, ocultação de dados, criptografia e esteganografia. A criptografia, na qual, 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, podendo ser 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. Os principais objetivos deste trabalho incidem em efetuar uma análise bibliográfica sobre os conceitos de esteganografia, pesquisar os softwares de perícia forense digital, comparar e relatar as diferenças dos arquivos originais dos modificados, identificando as vantagens e desvantagens da utilização das técnicas. A metodologia utilizada consiste em aplicar as análises de esteganografia nas imagens em diversas extensões, como JPEG, PNG e BMP, e dimensões, de 256, 512, e 1024 pixels, através dos softwares Kali Linux, Computer Aided Investigative Environment (Caine), Helix3 e Forense Digital ToolKit (FDTK).

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