Da Computação Forense a Técnica de Esteganografia. Um ensaio sobre a ocultação de informações em sistemas computacionais.

Mariana Pompeo Freitas, Wilson Jacobsen, Gustavo Rotondo, Daniela Almeida, Leonardo Pinho, Érico Amaral

Engenharia de Computação, Universidade Federal do Pampa (Unipampa)

Caixa Postal 96400-000 – Bagé – RS – Brazil

{maripompeof, willl.jacobsen,danilinalmeida}@gmail.com,
gustavo_.rotondo@hotmail.com,{leonardo.b.pinho, erico.amaral}@unipampa.edu.br

Abstract. *This paper presents extracts from a survey on Computer Forensics and its features. The aim is to present some methods of hiding data in files and recognized techniques for investigating environments corrupted by the methods of steganography. To achieve the objectives of this work were proposed and implemented experiments with different tools like outguess, and wbSteg Spammiminc. Preliminary results indicate the possibility of technical steganography operated by inexperienced users in the field of computer forensics, in addition to showing the validity of such tools for hiding information in computer systems.*
Keywords: *computer forensics, steganography*

Resumo. *Este artigo apresenta o extrato de uma pesquisa sobre a Computação Forense e suas características. O intuito é apresentar alguns métodos de ocultação de dados em arquivos e, técnicas reconhecidas para investigação de ambientes corrompidos pelos métodos de esteganografia. Para atingir os objetivos desse trabalho foram propostos e implementados experimentos com diferentes ferramentas como Outguess, wbSteg e Spammiminc. Os resultados preliminares apontam a possibilidade da técnica de esteganografia ser explorada por usuários inexperientes na área de forence computacional, além de mostrar a validade de tais ferramentas para a ocultação de informações em sistemas computacionais.*
Palavras-chave*: computação forense, esteganografia*

1. Introdução

Com o rápido desenvolvimento da computação e a popularização da internet, os sistemas computacionais e a tecnologia da informação se tornaram importantes e benéficas em várias atividades exercidas pelo ser humano. Neste contexto Dantas (2011) afirma que a informação tem adquirido um potencial de valoração para as organizações e para as pessoas. Nunes *et. al.* (2010) complementam descrevendo que a informação é posicionada como ativo estratégico determinante para o sucesso das empresas e que por isso, as instituições dependem de um sistema de informações de qualidade. Entretanto além dos aspectos positivos deste panorama, muitas vulnerabilidades podem ser encontradas o que estimula a prática de atividades ilícitas ou crime cibernéticos, definidos pela Symantec®(2014) como qualquer delito em que tenha sido utilizado um computador, uma rede ou um

dispositivo de hardware.

Toda a atividade ilícita cometida usando o computador deixa rastros ou dados que podem ser analisados na busca pelo criminoso. Assim como a investigação de crimes convencionais exige o recolhimento de provas (físicas), os cometidos por computador também exigem, nesse caso provas eletrônicas, porém estas são difíceis de recolher e preservar e, fáceis de destruir e alterar. Portanto o recolhimento destes indícios deve ser feito com base em cuidados específicos e por pessoas qualificadas. Esse conjunto de processos, que buscam garantir a integridade e veracidade das provas, é reconhecido como Computação Forense (CF). Para Rongsheng & K.P, (2011), a CF tem a finalidade de identificar, proteger, extrair e arquivar evidências eletrônicas, as quais possuem peso documental, para serem utilizadas em Juízo. Os autores esclarecem, ainda, que é importante coleta de evidências em curto prazo de tempo, a fim de garantir que integridade das mesmas. No âmbito da investigação forense, existem técnicas complexas e eficientes, que permitem a ocultação de informações em diferentes tipos de mídias ou arquivos, método conhecido como esteganografia. Ao identificar a importância da análise de todos dados possíveis, no caso da ocorrência de um incidente de segurança, este trabalho objetiva realizar uma revisão sobre Forense Computacional, com o foco em técnicas de esteganografia.

A estrutura adotada neste artigo é composta de 7 seções organizados da seguinte forma: na seção 2 será apresentado os referenciais teóricos que serviram de base para esse documento; na seção 3 temos os trabalhos correlatos; a metodologia está na seção 4; na seção 5 é apresentada a implementação, onde são descritos todos os experimentos e as ferramentas utilizadas nesse estudo; na seção 6 temos os resultados e discussões; por fim na seção 7 são apresentadas as conclusões preliminares desta pesquisa.

2. Referencial Teórico

Para embasar a proposta deste artigo faz-se necessário um levantamento teórico de aspectos relevantes ao tema, os quais são apresentados nesta seção, iniciando pelo levantamento sobre conceitos básicos de segurança, investigação em computação, forense computacional, esteganografia e trabalhos correlatos.

2.1. Segurança em Sistemas Computacionais

Campos (2007) afirma que um sistema de segurança da informação baseia-se em 3 princípios: confidencialidade, integridade e disponibilidade, eles nos dizem de forma resumida que somente pessoas autorizadas devem ter acesso a informação, que essa deve estar sem alterações, salva as autorizadas pelo proprietário e a informação deve estar sempre disponível, se um ou mais desses princípios forem desrespeitados, temos um incidente de segurança. Além disso, é importante ficar atento a técnicas utilizadas para roubo de informação, essas técnicas, geralmente estão ligadas a descoberta e exploração de vulnerabilidades, característica de um sistema que o torna sensível a certos ataques, Zúquete (2010). Um ataque é um conjunto de passos executados no âmbito da exploração de vulnerabilidades e que permitem concretizar uma ação ilícita. Um risco ou ameaça é o dano que pode resultar da execução bem sucedida de um ataque. A defesa consiste no conjunto de políticas e

mecanismos desenhados, concretizados e implantados para (i) diminuir as vulnerabilidades de um sistema, (ii) detectar e contrariar/anular ataques passados ou atuais e (iii) minimizar os risco decorrentes de ataques bem sucedidos. Geralmente quando um sistema computacional está sob ataque, esse começa a perder desempenho, já que seus recursos estão sendo comprometidos por hackers ou malwares. Ressalta-se que nos dias de hoje, os ataques estão cada vez mais frequentes como mostra a Figura 01 fornecida pela CERT[1], o que acaba agravando ainda mais o problema.

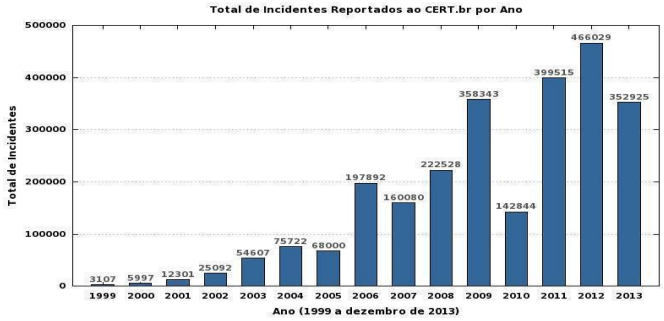

Figura 01: Incidentes reportados de 1999 à 2013.

Observa-se que do ano de 1999 até 2013 houve um crescimento de 11359% no total de incidentes reportados. Com o objetivo de investigar esses incidentes temos a atuação da computação forense que busca coletar evidências, identificar os atacantes e o modus operandi desses, a fim de se pensar em ações bem fundamentadas para garantir proteção contra novos ataques.

2.2 Investigação em Computação

Ao se tratar sobre investigação em sistemas computacionais é importante reconhecer que um computador pode ser utilizado como ferramenta de apoio à prática de delitos convencionais ou como um meio para a realização do crime, segundo Eleutério & Machado (2011), no primeiro caso o computador é usado como uma ferramenta auxiliar para realizar o ato ilícito, cita-se por exemplo a sonegação fiscal, a falsificação de documentos entre outros, já no segundo caso o computador é determinante para a execução do crime, é aqueles casos em que o crime não aconteceria se o dispositivo não existisse, alguns exemplos desse tipo de crime é citado por Wendt & Jorge (2013) como ataques a sites (Deface), roubo de informações e senhas através de engenharia social e malwares que seriam os softwares maliciosos (vírus, cavalo de tróia, rootkit, keylooger, botnets, etc) bem como o compartilhamento e/ou posse de arquivos de pornografia infanto-juvenil. Brassanini *et. al.* 2011 destacam, ainda, uma outra modalidade na qual o computador é uma de depósito de provas, que podem estar contidas em arquivos, e-mail e chats com cúmplices em relação a outros crimes como: homicídio, roubo de residências e tráfico de drogas. Em um local de crime, busca-se vestígios digitais, definidos por Franco (2012), como zeros e uns, dados lógicos que compõem a evidência digital, a qual poderá ser desde conversas em chats, histórico de internet, programas a arquivos excluídos intencionalmente pelo criminoso, para coletar essas evidências, é importante identificar e após, selecionar e coletar os equipamentos necessários. Destaca-se que durante esses procedimentos alguns

[1] CERT: Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Site oficial: http://www.cert.br/

cuidados especiais devem ser tomados, pois qualquer intervenção humana ou do próprio ambiente (impacto, umidade, calor excessivo) pode alterar, danificar ou destruir tais evidências. Esses cuidados incluem: A coleta deve ser feita por um especialista, no caso perito de informática que possua formação acadêmica e conhecimentos específicos; Não deixar pessoas estranhas usarem os equipamentos sem a supervisão de um perito; Não ligar equipamentos que estejam desligados, e; Em alguns casos, a ser analisado e decidido pelo perito, se os computadores estiverem ligados, pode-se interromper as conexões de rede e copiar dados da memória RAM com ferramentas próprias pra isso, pode-se ainda analisar os processos que estão em execução no momento. Ainda, segundo Eleutério & Machado (2011), os dispositivos computacionais só devem ser apreendidos se há desconfiança de que eles podem conter evidências necessárias para investigação, nesse caso, é decisão do perito apreender o gabinete inteiro, ou apenas os discos rígidos bem como os demais equipamentos eletrônicos e dispositivos de armazenamento (telefones celulares, tablets, GPS, câmeras, CD's, DVD's, pendrives, etc). A *International Organization on Computer Evidence* (IOCE, 2002) cita que todas as provas apreendidas (inclui-se equipamentos suspeitos de conter provas) devem ser devidamente embaladas e lacradas e que todas as atividades relativas à apreensão, acesso, armazenamento ou transferência de evidências digitais devem ser devidamente documentados, preservados e disponíveis para análise além disso, diz que, sempre que possível, os itens apreendidos devem ser examinados no laboratório ou espaço de trabalho forense em vez de no local do crime. Isso é compreensível já que tal espaço deve estar equipado para o exame. Essas ações são base para a técnica conhecida como computação forense.

2.3 Computação Forense.

Para G. Pangalos *et. al.* 2010, a Computação Forense é definida pela busca e coleta de evidências, em sistemas computacionais, por meio de técnicas padronizadas e devidamente documentadas, resultando desta maneira em dados com valor probatório. A CF segue 4 etapas, os quais são descritos na figura 02.

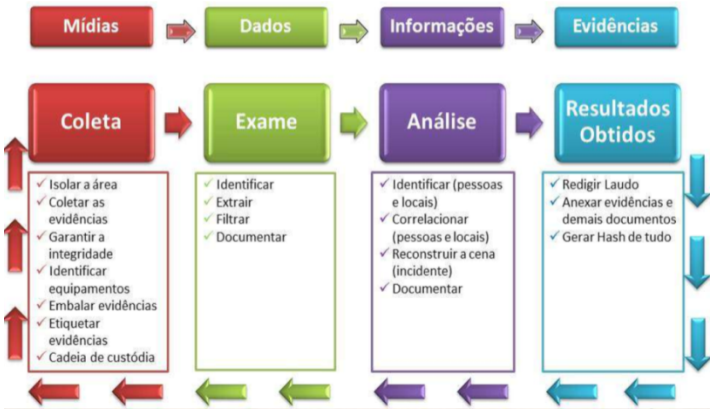

Figura 02: Etapas Forense Computacional, FDTK (2012)

Como etapa inicial, tem-se a coleta do equipamento violado e o posterior registro, bit-a-bit, de as todas informações contidas no computador, contemplando desde o sistema operacional até os

demais dados armazenados. O processo de exame das cópias é realizado após esta fase, por meio da duplicação das informações, a qual pode ser realizada com a utilização de bloqueadores de escrita, aparelhos de proteção contra gravação de dados que tem o objetivo de evitar a alteração dos mesmos. Na etapa de análise, Robert *et. al.* (2009), indicam a adoção de ferramentas apropriadas para essa tarefa, com o intuito de documentar os procedimentos utilizados e resultados encontrados. Por fim, a ultima fase é caracterizada pela emissão de laudos e anexo das evidências apuradas. Ainda em relação a etapa três da CF, podem ser apresentadas como exemplos de ferramentas para análise de sistemas corrompidos: o Caine (*Computer Aided Investigative Environment*), uma distribuição linux italiana, que oferece um ambiente completo para todas as fases de investigação digital (http://www.caine-live.net/); o FDTK Ubuntu, ferramenta sobre a plataforma Linux, que reúne mais de 100 ferramentas capazes de atender a todas as etapas de uma investigação em Forense Computacional (http://fdtk.com.br/www/sobre/). Exemplos para ambientes Windows, especificamente são: a *Forensic Acquisition Utilities* (FAU), uma coleção de utilitários e bibliotecas destinados a utilização de investigação forense (http://gmgsystemsinc.com/fau/); o Encase, aplicação que auxilia em todas as fases da investigação, é capaz de fazer uma cópia completa, de maneira totalmente não-intrusiva, dos das informações presentes no dispositivo suspeito, gerando um arquivo de evidências (http://forensedigital.com.br/product/encase-forensic-v6/).

A partir do reconhecimento das fases, definidas para a forense computacional e, das ferramentas disponíveis para esta finalidade é possível descrever as ações possíveis para a avaliação de um incidente: Verificar a existência de rootkits, senhas e arquivos na imagem de memória; Identificar possíveis arquivos apagados; Descobrir senhas contidas na memória; Verificar os pacotes que estão em trânsito, as conexões e portas abertas e possíveis portas TCP/UDP ocultas; Analisar logs, memória swap, diretórios, sistema operacional, arquivos em qualquer formato suspeitos. Os arquivos podem conter dados ocultos, por meio de esteganografia e esconder dados importantes, essa é uma técnica anti-forense (métodos e formas de remoção e ocultação de evidências).

2.4. Esteganografia

Segundo Johnson & Jajodia, 1998, a esteganografia é a arte de esconder informações de forma a evitar a detecção de mensagens escondidas, deriva do grego e significa "escrita coberta". Essa não é uma área nova, muitas técnicas são conhecidas a milhares de anos, um exemplo comentado por Rocha (2003), descreve que na Grécia Antiga eram usados tabletes de madeira cobertos com cera, onde escreviam-se mensagens e cobriam-se com cera, a fim de simular um tablete de cera normal.

Atualmente as técnicas de esteganografia são praticadas usando tecnologia como descrito por Chen Ming et al escondendo a mensagem secreta incorporando-a em textos, imagens, áudios, vídeos ou outras mídias digitais. O objetivo hoje ou anos atrás continua o mesmo, fazer com que os dados não sejam percebidos por terceiros. Tendo em vista este objetivo, a análise de arquivos em computadores apreendidos é importante, pois pode revelar provas de crimes. Um exemplo real desta técnica é o caso do traficante Juan Carlos Abadia, que transmitia ordens para seu cartel de drogas, por meio de imagens via mail, de forma oculta. Uma das técnicas que permitem a ocultação de dados em imagens é conhecida como LSB (*least significant bits*), consistindo em usar os bits menos significativos de cada

pixel da figura, para ocultar mensagens, se tornando imperceptível. Além desta, outras técnicas possibilitam a inserção de dados em arquivos, tais como filtragem e mascaramento, as quais exploram as modificações nos bits mais significativos da imagem, com o uso de algoritmos e transformações.

Além do fato que evidências de um delito podem estar ocultas dentro de arquivos, a esteganografia também pode ser usada para ocultar vírus, em 2011 foi divulgado no site do G1 um vírus chamado "Alureon" descoberto pela Microsoft (2011). Esta aplicação maliciosa realizava o upload de fotos em blogs, as quais de forma oculta, continham instruções para o vírus, incluindo o endereço dos servidores de controle. Como resultado do ataque, o Alureon passava o controle do sistema para o atacante. Vale citar que a esteganografia pode ser usada para evitar violação de direitos autorais (marca d'agua digital) mas, para fins desse artigo abordamos o assunto partir de uma perspectiva do criminoso e do investigador.

3. Trabalhos Correlatos

Adicionalmente ao referencial teórico, nesta seção são apresentados três trabalhos correlatos, relacionados ao tema de pesquisa descrito neste artigo.

A pesquisa intitulada *"The Study of Computer Forensics on Linux",* por Tang (2013) apresenta os conceitos da computação forense e descreve alguns métodos utilizados para preservação de evidências e recuperação de dados usando como mecanismo o sistema operacional Linux.

O artigo *"An Introduction to Image Steganography Techniques",* por Altaay et al (2012) mostra uma visão geral da esteganografia de imagem, bem como apresenta algumas características que um algoritmo de esteganografia deve possuir para obterem sucesso na incorporação de dados.

O trabalho "*Stego-Analysis Chain, Session Two Novel Approach of Stego-Analysis System for Image File*", por Naji el al (2009) apresenta um estudo sobre identificação de dados ocultos em imagens e o seu impacto na textura.

4. Metodologia

Este estudo vislumbra, a partir de uma pesquisa bibliográfica sobre o tema esteganografia e forense computacional e, um levantamento de ferramentas específicas para CF, apresentar técnicas para ocultação de dados dentro de diferentes arquivos, bem como apresentar métodos para detecção e investigação de alguns arquivos. Um infográfico, representado na figura 03, apresenta as etapas definidas para este estudo.

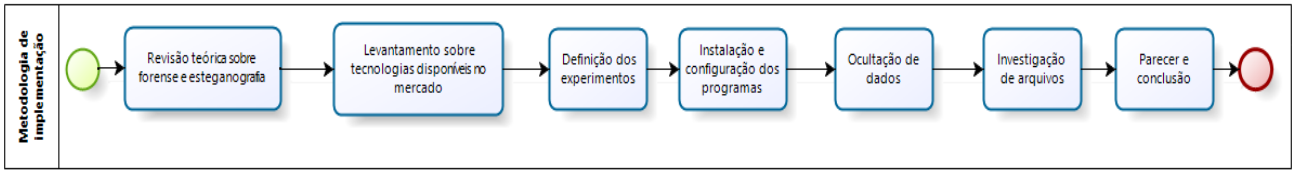

Figura 03: Etapas adotadas na pesquisa

Para alcançar o objetivo delineado serão realizados experimentos sobre diversas ferramentas, usando diferentes sistemas operacionais, com o intuito de estudar e trabalhar com diferentes softwares para a

identificação de diferentes possibilidades de análise. Nesse trabalho é utilizado, como plataforma para os testes, o sistema operacionais FDTK e Windows XP, justificado por: O FDTK possuir um número significativo de programas voltados a esteganografia, em comparação a outros sistemas gratuitos, voltados a forense; O Windows XP, devido a sua utilização em larga escala por usuários finais e pelo suporte a aplicação Wbstego.

5. Implementação

Para a realização dos experimentos desse estudo, foram instaladas as plataformas FDTK e Windows XP. Em relação a instalação das ferramentas, as aplicações Outguess, Stegcompare e Xsteg são nativas do FDTK, o que não não gerou a necessidade de instalação, enquanto a ferramenta wbStego foi instalada no Windows XP. Este software foi elencado, porque permite ocultar diversos tipos de conteúdos em arquivos. Salienta-se que também foram realizados testes para a inoculação de informações em arquivos utilizando o shell do windows. Por fim, a ferramenta Spammimic, uma solução online, também foi avaliada. Em um primeiro momento são realizados os testes de ocultação de arquivos, após os testes de detecção e investigação sobre os arquivos corrompidos. Todos os experimentos foram realizados sem o uso de senha.

Experimento 1: usando o Prompt de Comando:

Envolveu 2 imagens (imagem1.jpg e imagem2.jpg) e 1 arquivo txt, compactou-se a imagem1 e o arquivo texto (usando o Winrar). No prompt digitou-se o seguinte: *copy /b imagem2.jpg + arqCompactados.rar imagem3.jpg* Dessa forma, foi gerado um arquivo (imagem3.jpg) com dois arquivos ocultos.

Investigando: O perito deve analisar todos os arquivos do computador, nos suspeitos deve ver se há como extrair algum conteúdo.

Experimento 2: usando o Outguess

Para esconder o conteúdo em uma imagem, abriu-se o programa no FDTK e digitou-se o comando: *outguess -d nome_do_arquivo.txt nome_da_imagem.jpg outro_nome_imagem.jpg* . Assim "escondeu-se" o arquivo txt dentro de uma imagem e gerou-se uma outra imagem (outro_nome) com o conteúdo oculto.

Investigando: Para descobrir arquivos ocultos usando esse mesmo programa, digitou-se o seguinte comando: *outguess -r outro_nome_imagem.jpg outro_nome_arquivo.txt* Dessa forma extraiu-se o conteúdo da imagem suspeita (outro_nome_imagem) e gerou-se um outro arquivo txt (outro_nome_arquivo) com o contéudo que estava oculto. Depois, usou-se a ferramenta Stegcompare, também disponível no FDTK para comparar as duas imagens (original x com conteúdo oculto), digita-se: *stegcompare imagemoriginal.jpg imagemmodificada.jpg* , o programa nos retornou que os tamanhos das imagens eram diferentes, o que pode indicar ao perito uma esteganografia. Uma outra ferramenta usada na investigação dos arquivos gerados no Outguess foi o xsteg acessado. Esse software detecta esteganografia em arquivos JPG de um determinado diretório, seleciona-se o diretório (Desktop, Documentos entre outros) e o programa analisa todos os arquivos JPG disponíveis no local. Uma observação interessante feita durante o experimento é que essa ferramenta é capaz de analisar

imagens que estavam no diretório escolhido mas que foram “excluídas” e encontram-se na lixeira.

Experimento 3: usando o wbStego

Foi realizado o download através do site oficial do projeto http://wbstego.wbailer.com/, nesse mesmo site é possível baixar o software para Linux. Nessa ferramenta ocultou-se texto dentro de imagem (BMP), imagem dentro de pdf, planilha (XML) dentro de pdf, texto dentro de planilha e imagem (JPEG) dentro de outra (BTM).

Investigando: Pode-se extrair o arquivo oculto usando esse mesmo programa, selecionando no inicio Decode e posteriormente, os arquivos suspeitos para terem o conteúdo extraído. A técnica de ocultar uma imagem dentro de outra pode ser usada por exemplo, para esconder imagens de pedofilia dentro de outras aparentemente inocentes.

Experimento 4: usando o Spammiminc:

Essa é uma ferramenta online de esteganografia de texto, ou seja, que oculta um texto dentro de outro. Basta acessar o site: http://www.spammimic.com/ Escrevemos a frase: “Me encontre na universidade.” e obtemos um texto, segue-se uma amostra do mesmo:

“ Dear Friend , This letter was specially selected to be sent to you ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 1621 ; Title 1 ; Section 307 ! This is different than anything else you've seen !

A mensagem é disfarçada de forma que se parece com um spam. Segundo Vitaliev (2009), esse texto gerado no site é uma fórmula de palavras intercambiáveis, ou seja que podem ser trocadas sem que haja alteração do resultado, isso garante que o spam pareça autêntico. Pode-se copiar o texto gerado e enviar por e-mail ao destinatário, esse bastaria entrar no site e decodificar (*decode)*.

Investigando: observe que entre todas as palavras e pontuações há um espaço (tanto antes quanto depois dele), esse já seria um motivo para desconfiança de esteganografia, entre esses espaços pode conter algo oculto. Pode-se usar um editor hexadecimal para verificar a quantidade de espaços contidos. Caso o perito suspeite de algum e-mail ou arquivo de texto armazenado no computador, poderia optar por uma análise forense de redes, verificando o tráfego, ver no histórico os últimos sites acessados e caso seja detectado a página do Spammimic, bastaria colar o texto suspeito e decodificar como já foi explicado.

6. Resultados e Discussões

Durante a realização dos experimentos, mostrou-se que existem diversas ferramentas para ocultar diferentes tipos de arquivos dentro de outros, e que existem várias formas para a investigação desses.

No primeiro experimento não foi usado nenhuma ferramenta especifica de esteganografia, ou seja, não ter uma ferramenta instalada, não significa que não que não há evidências escondidas em arquivos. No segundo experimento só conseguiu-se trabalhar com arquivos jpg e texto, o que facilitou nossa análise forense, já que temos o xsteg que identifica esteganografia em arquivos jpeg. Nesse mesmo teste mostramos que se tivermos a imagem original e a que contém conteúdo oculto podemos compará-las (stegcompare) e dependendo do resultado, pode-se suspeitar do arquivo. No terceiro

experimento usou-se uma ferramenta interessante, pois permite a ocultação de diversos tipos de arquivos dentro de pdf, btm e xml. Nesse caso, usar o xsteg para identificar esteganografia de imagem não é eficiente porque o programa aceita para arquivo final somente o tipo btm e o xsteg analisa jpg. Mas fazendo uma pesquisa descobre-se técnicas que podem auxiliar na análise de arquivos btm, como os ataques aurais (retira-se partes significativas da imagem, como um meio para facilitar a busca por anomalias na imagem), ou os ataques estatísticos (usam os padrões de pixels e seus bits menos significativos para tentar revelar a mensagem oculta) esses ataques foram citados por Albuquerque et al (2007). Pesquisando também descobre-se técnicas e programas gratuitos para análise de pdf, como por exemplo o comando pdfinfo e outros para análise de xml. No último experimento usamos uma ferramenta online, e da mesma forma que o primeiro experimento vê-se que não é obrigatório programas instalados para a ocultação de dados, mas nesse caso é necessário ter acesso a internet, tanto para codificar quanto para decodificar, então fazendo uma busca nos históricos e verificando o tráfego pode-se detectar o acesso ao site da ferramenta, e daí suspeitarmos da técnica de esteganografia. Como citado na seção anterior nesse experimento também pode-se usar um editor hexadecimal e identificar a quantidade de espaços (20 em hexa) usados no texto suspeito, se houver muitos, é provável que tenha algo oculto dentro deles.

7. Conclusão

Com o decorrer deste estudo, vimos que durante uma análise forense computacional é importante que o perito verifique todos os arquivos e se há programas de esteganografia instalados no computador, se houver é grande a possibilidade de haver arquivos ocultos dentro de outros e que o programa encontrado tenha sido utilizado para esse fim, nesse ponto é interessante pesquisar e ver que tipos de arquivos (extensões) o programa pode esconder, e que tipos ele aceita para ser o arquivo final, isso facilita na busca pelos dados suspeitos, também mostramos através do experimento com prompt de comando que não ter uma ferramenta específica instalada, não significa que não tenha evidências ocultas dentro de outros arquivos. Percebeu-se durante o estudo a dificuldade com que o perito pode deparar-se na análise de arquivos, devido à quantidade de softwares de esteganografia existentes no mercado e os inúmeros tipos de arquivos que podem ser ocultos dentro de outros. Mas também verificamos que existem inúmeras técnicas e ferramentas disponíveis para investigação desses documentos.

Os objetivos desse trabalho foram alcançados, pois foi possível aplicar técnicas de ocultação de diferentes tipos de dados e apresentar algumas formas para investigação dos arquivos.

Referências

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, MÁRCIO Pereira . **Desvendando a Computação Forense**, Novatec, 2011.

CAMPOS, André. **Sistemas de Segurança da Informação**, 2ª edição, Visual Books, 2007.

Dantas, Marcus Leal. Segurança da Informação. Uma abordagem focada em gestão de riscos, Livro Rápido, 2011.

ZÚQUETE, André. **Segurança em Redes Informáticas**, 3ª edição, FCA, 2010.
BRASSANINI, David; MORENO Karine; Taxman. **Guia de Campo Sobre Prova Digital**, Federal Bureau of Investigation, 1ª ed. 2011.
RONGSHENG Xu; CHOW, K.P; YING, Yang. ***Development of Domestic and International Computer Forensics***. IEEE, 2011.
FRANCO, Deivison Pinheiro. **A Computação Forense e a Investigação de Crimes Cibernéticos – CSI do Século XXI**. Revista Convergência Digital, nº 2, 2012.
G. PANGALOS; C. Ilioudis; I. PAGKALOS. **The importance of Corporate Forensic Readiness in the information security framework**. IEEE, 2010.
JOHNSON, Neil F; JAJODIA, Sushil. **Exploring Steganography: Seeing the Unseen**. IEEE, 1998.
MING, Chen; RU, Zhang; XINXIN, Niu; YIXIAN, Yang. **Analysis of Current Steganography Tools: Classifications & Features**. IEEE, 2006.
TANG Ling. **The Study of Computer Forensics on Linux**. IEEE, 2013. Alaa A Altaay. Jabbar; SAHIB, Shahrin bin; ZAMANI Mazdak. **Introduction to Image Steganography Techniques**. IEEE, 2012.
ROBERT Lee; SHEAU-Dong Lang; KEVIN Stenger. **From Digital Forensic Report to Bayesian Network Representation**. IEEE, 2012.
NAJI, A.W.; HAMEED, S.A.; ISLAM, M.R.; ZAIDAN, B.B.; GUNAWAN, T.S.; ZAIDAN, A.A . **Stego-Analysis Chain, Session Two Novel Approach of Stego-Analysis System for Image File**. IEEE, 2009.
VITALIEV, Dmitri. **Manual de Seguridad y Privacidad Digital Para Los Defendores de Los Derechos Humanos**, FrontLine - International Foundation for the Protection of Humans Rights Defenders, 2009.
ALBUQUERQUE, Célio; Julio, Eduardo PAGANI; Brazil, Wagner Gaspar: Fonte (2007)
WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos, Ameaças e Procedimentos de Investigação**, 2ª edição, Brasport, 2013.
GBP. **Guidelines for Best Practice in the Forensic Examination of Digital Technology. International Organization on Computer Evidence**, 2002.
____ http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_digit_tech.html#AimsGoals
____ http://www.fdtk.com.br/files/Minicurso_Forense-2012-1.pdf
____ http://g1.globo.com/tecnologia/noticia/2011/09/virus-esconde-configuracoes-de-operacao-em-foto-de-tom-cruise.html
____ http://www.caine-live.net/
____ http://fdtk.com.br/www/sobre/
____ http://gmgsystemsinc.com/fau/
____ http://forensedigital.com.br/product/encase-forensic-v6/
____ http://www.techpathways.com/prodiscoverdft.htm
____ http://br.norton.com/cybercrime-definition