UNIVERSIDADE SAGRADO CORAÇÃO

Centro de Ciências Exatas e Sociais Aplicadas

Bacharelado em Ciência da Computação

THIERRY DE OLIVEIRA CIARAMICOLO

ANÁLISE DE FERRAMENTAS DE APOIO A PERÍCIA FORENSE COMPUTACIONAL

BAURU

2011

THIERRY DE OLIVEIRA CIARAMICOLO

ANÁLISE DE FERRAMENTAS DE APOIO A PERÍCIA FORENSE COMPUTACIONAL

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título de Bacharel em Ciência da Computação, sob orientação do Prof° Dr. Kelton Costa.

BAURU

2011

Thierry de Oliveira Ciaramicolo
Análise de ferramentas de apoio à perícia forense computacional.
Thierry de Oliveira Ciaramicolo - 2011
36 p.
Orientador: Prof° Dr. Kelton Costa
Trabalho de Conclusão de Curso (Ciência da
Computação) - Universidade do Sagrado Coração -
Bauru - SP.
1. Perícia Forense Computacional 2.
Legislação e Informática 3. Engenharia Social 4.
Ciência da Computação I. Prof° Dr. Kelton Costa
II.Título

THIERRY DE OLIVEIRA CIARAMICOLO

ANÁLISE DE FERRAMENTAS DE APOIO A PERÍCIA FORENSE COMPUTACIONAL

Trabalho de Conclusão de Curso apresentado ao Centro de Ciências Exatas e Sociais Aplicadas como parte dos requisitos para obtenção do Título de Bacharel em Ciência da Computação, sob orientação do Prof. Kelton Costa.

BANCA EXAMINADORA

_____

Prof° Dr. Kelton Costa

Orientador

_____

Prof° Esp. Henrique Pachioni Martins

Examinador

_____

Prof° Mestre Wiliam Carlos Galvão

Examinador

DATA: 13/06/2011

AGRADECIMENTOS

A **Universidade do Sagrado Coração - USC**, instituição que sempre prezou pela qualidade de ensino.

Aos meus pais **Walter Ciaramicolo e Ondina Soares de Oliveira Ciaramicolo**, pelo apoio na realização deste trabalho.

Aos **professores do curso de Ciência da Computação**, todos sempre muito presentes e cumpridores de seus deveres.

Em especial aos professores **Kelton Costa**, **Henrique Martins**, **Elvio Gilberto** pela ajuda obtida não só neste trabalho mas no decorrer de todo o curso e pelo grande serviço realizado em benefício do curso de Ciência da Computação ao longo destes anos.

Aos meus amigos **Denise Carrozza Bedollo, Fulvia Salandini, Profª Raquel Sanzovo, Victor Eduardo Slompo**, que me auxiliaram na conclusão deste trabalho.

RESUMO

Este trabalho tem como objetivo esclarecer o presente contexto referente a pericia forense computacional, demonstrando quais são as leis referentes ao crimes digitais, o papel do perito forense computacional, a concepção de engenharia social, destacando sua grande utilidade na realização de certos crimes, a importancia da segurança da informação, uma analise das ferramentas utilizadas pelos criminosos para tentar burlar a segurança imposta por empresas e pessoas. Será também neste trabalho exibido algumas das ferramentas periciais, utilizadas para aquisição de provas contra criminosos, fundamentais na elaboração de um processo criminal, além da explicação da técninca de esteganografia, uma maneira muito eficaz de ocultar mensagens.

ABSTRACT

This study aims to clarify the present context refers to computer forensics expertise, showing what are the laws regarding computer crimes, the role of expert computer forensics, the conception of social engineering, emphasizing its great usefulness in certain crimes, the importance information security, an analysis of the tools used by criminals to try to circumvent security imposed by companies and individuals. Does this work also show some of the forensic tools used for acquiring evidence against criminals, underlying in preparing a criminal case, also an explanation of steganography technics, a very effective way to hide messages.

LISTA DE ABREVIATURAS

HD – Hard Disk

HTCIA - High Technology Crime Investigation Association

HTML - Hypertext Markup Language

IOCE - International Organization on Computer Evidence

LSB - Least Significant Bit

SIM – Subscriber Identity Module

WINDOWS LIVE ID - Sistema de Autenticação de Usuários Microsoft

XML- eXtensible Markup Language

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Nos dias atuais se torna cada vez mais dependente o ser humano de suas máquinas, empresas privadas, órgãos do governo, escolas, pequenos empreendimentos, residências, todos tem algo em comum, a crescente dependência dos computadores. Esta dependência devido às facilidades trazidas pode parecer inofensivas, mas basta um simples problema de ordem técnica e uma instituição pode estar arruinada, caso esta não esteja preparada.

Quando se pensa na fragilidade de um sistema computacional, um fato se torna marcante, se mesmo isolado o mesmo já é vulnerável, aquele com uma conexão via internet se torna ainda mais, pois toda pessoa em qualquer parte do mundo, com más intenções, conhecimento e uma conexão com a internet, pode gerar problemas.

Por estes intentos que se ressalta um aspecto interessante da internet, o fato de que a mesma cria uma sensação de impunidade ao criminoso, pois muitas vezes ele comete um crime a quilômetros de distância, acreditando que nunca será pego, que não existem formas de ser encontrado, pois ele não passa de mais um computador na rede com milhões de outros, mas isto nem de perto é verdade.

Muitas pessoas acreditam que o computador traz segurança e anonimato, crenças estas que podem ser prejudiciais tanto aqueles que utilizam o computador e a internet para um uso correto e responsável, tanto para aquele que os utiliza para cometer crimes, pois de forma alguma a anonimato está garantida.

Vale ressaltar que mesmo os crimes digitais terem seus aspectos diferentes dos crimes tradicionais, estes são totalmente passiveis de punição, pois se encaixam perfeitamente nos crimes ja previstos por lei, alterando-se apenas o fato que a presença do criminoso no local não existe fisicamente.

É de conhecimento geral o fato de que funcionários descontentes, pessoas com tempo sobrando, intenções ruins e conhecimento na área da informática, pedófilos, estelionatários, enfim, todo tipo de pessoa má intencionada cresce na rede.

Para conseguir coibir e punir os criminosos se faz necessário um profissional adequado para cada tipo de crime, no caso dos crimes envolvendo informática, o profissional responsável por isto é o perito forense, pois ele encontrará os vestígios deixados pelos criminosos, afim de encontrados e elaborar um processo judicial firme, que possa levá-los a condenação.

Toda atividade em um computador, rede ou cyber espaço, deixa vestígios, mesmo arquivos que estariam teoricamente apagados podem ser recuperados, se procurados da maneira certa, no lugar certo e no tempo certo.

A falta de profissionais na área de perícia forense computacional leva muitas pessoas a saírem impunes de crimes cometidos contra pessoas ou empresas.

> Quando o assunto é segurança da informação, os maiores riscos para as empresas são represálias de ex-funcionários e a ausência de recursos adequados para uma preparação adequada. Esta é a conclusão do 12º estudo anual da Ernst & Young sobre Segurança da Informação, realizado em âmbito global. A represália de ex-funcionários contra seus ex-empregadores é o motivo de maior preocupação para 75% dos gerentes de TI. (ERNST & YOUNG, 2011, n.p.).

Entender que para este tipo de crime acontecer muitas vezes não basta apenas a astucia e conhecimento do criminoso, mas também a falta de preparo e até mesmo uma "inocência" por parte dos responsáveis da segurança do sistema.

Utilizando-se de pesquisa bibliográfica, este trabalho tem primeiramente como objetivo esclarecer do que se trata a pericia forense, mais especificamente sobre a pericia forense computacional, de onde são obtidas as provas e como obtê-las, para que sejam apresentadas de maneira confiável em um processo judicial.

1.1 Objetivos Gerais

Tomando como ponto de partida a pesquisa forense, para tal, o objetivo do trabalho foi, esclarecer do que se trata a pericia forense, mais especificamente sobre a perícia forense computacional, demonstrar quais são os crimes digitais, qual o papel do perito computacional, mostrar as técnicas utilizadas pelos criminosos na obtenção de acesso a dados privados, realizar uma análise de alguns softwares ligados a pericia forense computacional.

1.2 Objetivos Específicos

Os Objetivos Específicos foram:

- Explicar o que é pericia forense, e o que é pericia forense computacional.
- Mostrar as leis que abrangem os crimes de informática.
- Mostrar os programas e técnicas usadas pelos criminosos.
- Entender o que significa segurança da informação.

- Conhecer os programas e técnicas utilizadas na pericia forense computacional.

1.3 Justificativa

Devido à pericia forense computacional ser uma área extremamente nova, faz-se necessário o desenvolvimento de trabalhos que visam esclarecer a forma de trabalho do perito, suas técnicas e programas utilizados na captura dos criminosos.

Também é necessário saber quais são as técnicas usadas pelos criminosos, para realizar um trabalho eficiente, tanto na localização dos criminosos, quanto na obtenção de provas.

Além disso, deve-se conhecer quais são os crimes digitais, qual o papel do perito computacional, mostrar as técnicas utilizadas pelos criminosos na obtenção de acesso a dados privados, assim como as técnicas utilizadas para solucionar os crimes e recuperar dados quando estes forem danificados.

1.4 Estrutura do Trabalho

Em um primeiro momento, será mostrado o conceito, não só de pericia forense, e sim mais especificamente de pericia forense computacional, definindo também quem são os peritos e quais suas funções.

Em seguida, descrito o que é e a importância da segurança da informação, além de uma breve explicação sobre firewall, virus, trojan e outras técnicas de segurança e de ataque mais utilizadas.

Na continuação virá o assunto engenharia social, que mesmo sendo uma das técnicas usadas pelos criminosos para conseguir acesso a certas informações, ela não trata exatamente da utilização de um software, mas sim algo mais relacionado a uma atuação por parte do criminoso.

E posteriormente serão demonstradas as ferramentas utilizadas pelos peritos forenses computacionais e as considerações finais.

2 FUNDAMENTOS EM PERÍCIA FORENSE COMPUTACIONAL

O termo perícia, do latim *peritia*, significa habilidade, saber. Na linguagem jurídica significa a pesquisa, o exame, a verificação acerca da verdade ou da realidade de certos fatos.

A perícia forense aplicada à informática, também referenciada como computação forense, forense computacional, criminalística computacional, forense digital, investigação eletrônica e perícia eletrônica, é a aplicação de conhecimento em informática de técnicas de investigação com a finalidade de obtenção de evidências de crimes digitais.(PIMENTA, 2007, p.14)

A perícia tem como espécies: os exames, as vistorias e as avaliações. Todas se dizem, genericamente, Exames Periciais. É pois meio de prova, conforme o disposto no caput do art. 420 do Estatuto Processual: "Art. 420. A prova pericial consiste em exame, vistoria ou avaliação." (DE PAULA, 2003, n.p.).

Quando procura-se algo especifico, as chances de encontrá-lo são bem menores. Porque, entre todas as coisas no mundo, está procurando apenas uma. Ao procurar qualquer coisa, suas chances de encontrá-las são bem maiores. Já que, entre todas as coisas no mundo, você tem a certeza de encontrar alguma delas (DARRY ZERO apud FARMER, 2006, p.3).

Segundo Theodoro, o estatuto processual classifica a perícia em:

> 1- Exame: é a perícia propriamente dita, pois consiste no trabalho que o perito faz de inspecionar coisas ou pessoas, procurando desvendar os aspectos técnicos ou científicos que, ocular mente, não se encontram visíveis.
> 2- Vistoria: trata-se da mesma atividade do Exame, mas restrita aos bens imóveis;
> 3- Avaliação: é a atribuição de valores para bens jurídicos (direitos, obrigações, coisas). (Theodoro, 2003, n.p.)

Theodoro ressalta, ainda, que a perícia possa ser classificada em:

> a) Judicial: a que ocorre dentro do processo, com perito nomeado pelo juiz.
> b) Extrajudicial: parecer técnico apresentado pela parte (autor e/ou réu), instruindo a inicial e a contestação, a fim de se evitar a perícia judicial.
> c) Informal: espécie de perícia judicial, onde o laudo é dispensado. Pode o juiz inquirir o perito e assistentes técnicos acerca do que verificaram, sem o formalismo do laudo. (Theodoro, 2003, n.p.)

Da necessidade do avanço científico, e utilizando-se do conceito de perícia forense, surge uma ciência para garantir que a manipulação dessas novas formas de evidências eletrônicas fosse aceitas em juízo: A análise forense computacional. (BARROS, 2009). Segundo o mesmo autor, a análise forense computacional

> compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.(BARROS, EDUARDO, 2009, p.12)

As provas "podem ser as mais diversas possíveis como *e-mails*, arquivos de registros (conhecidos como *logs*), arquivos temporários com informações pessoais, conexões abertas, processos em execução" e, além disso, toda e qualquer "evidências que possam existir na máquina, mas para serem aceitas num processo jurídico, devem ter sido obtidas de forma lícita." (TREVENZOLI, 2006, p.11)

As provas de crimes digitais, como quaisquer outras provas, devem ser autênticas, exatas, completas e precisam convencer o júri ou a corporação e estarem em conformidade com a lei. (PIMENTA, 2007, p.15).

Por fim, "uma perícia em um computador suspeito de invasão ou mesmo um computador apreendido em alguma batida policial envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise" (BARROS, 2009, p.12) como nos aponta Barros (2009):

> Existe a necessidade de se conhecer minúcias do sistema operacional para que se tenha uma noção global de todos os efeitos das ações do perito.
> Quanto à necessidade de se utilizar ferramentas específicas para análise, esta decorre da obrigatoriedade de não se perturbar o sistema que está sendo analisado, perturbações essas que podem ser traduzidas como mudanças nos tempos de acesso aos arquivos anulando, assim, uma das mais poderosas formas de se reconstituir o que aconteceu na máquina em um passado próximo. Ferramentas convencionais não têm a preocupação de manter a integridade dos tempos de acesso.
> A "Cena do Crime" deve ser preservada para que provas não sejam acidentalmente modificadas ou perdidas." (BARROS, EDUARDO, 2009 p.12)

É importante, também, saber que o profissional responsável pela perícia forense é conhecido como perito. Esse profissional pode ser classificado em

> **Perito criminal:** São profissionais que prestaram concurso e fazem parte do quadro das polícias estaduais ou federais. (FREITAS, 2006, p.1)

> **Perito judicial:** Com conhecimento técnico e muita experiência profissional é designado pelo juiz para realizar a perícia. Deve ter conhecimento suficiente para montar um prontuário, ter conhecimento dos ritos processuais, além de maturidade. Na maioria das vezes é um profissional liberal que atua em outras atividades, não pode ter envolvimento com juízes ou com as partes do processo. (FREITAS, 2006, p.1)

Segundo Lau (2007) outra profissão de interesse a este trabalho é o Assistente Técnico, "especialista que pode ser nomeados pela partes do processo para criticar os laudos dos peritos, geralmente trabalha a favor do cliente e procura sempre manipular a técnica a favor do seu interesse, em vez de buscar a verdade".

Já o perito computacional (VIOTTO, 2010) pode atuar tanto na esfera pública – como funcionário da Polícia Federal, por exemplo – quanto na iniciativa privada, prestando consultoria para empresas que necessitem detectar possíveis delitos digitais. Os principais problemas dentro das companhias acontecem por conta de ações de funcionários ou ex-funcionários insatisfeitos.

Mais especificamente, o Perito deve se preocupar em registrar quem teve acesso as provas. A maneira mais simples é manter uma lista detalhada dos indivíduos que tiveram algum material apreendido sob seu poder, desde a apreensão até a devolução. Entre as informações relevantes que merecem ser anotadas estão a data e a hora da ação, a quem a pertencia o material ou quem forneceu, local da apreensão, descrição completa do material, de quem as provas foram recebidas (com data), a quem foram entregues (com data) e outras informações peculiares ao caso. (BARROS, 2009)

Deste modo, mesmo que o contraventor utilize um sistema de e-mail gratuito é possível rastrear os caminhos da mensagem e chegar à máquina de onde ela saiu. "Com um mandado de segurança, conseguimos informações do provedor de e-mail ou do fornecedor de internet", comenta ele. Milagre (2007) afirma que, às vezes, a investigação pára aí, pois a máquina usada pertence a um local público de acesso, um internet café ou uma lan house. "Mas com a nova lei, que exige que tais locais registrem seus usuários, esta prática se tornará mais difícil", acredita (VIOTTO, 2007).

Viotto (2007) ainda diz que, os peritos trabalham também na identificação de uso de software piratas nas empresas. Os infratores bem que tentam livrar-se das provas. "Uma vez, o acusado formatou a máquina cinco vezes na tentativa de apagar o rastro do registro ilegal de programas na máquina, mas temos ferramentas que permitem recuperar dados depois de até sete formatações", conta Milagre (2007, n.p.). Em outra ocasião, um dos computadores a foi atirado do quinto andar na esperança de que ele fosse danificado, mas também conseguimos restaurar os dados e provar a fraude.

Assim, vale salientar a importância de se conhecer um pouco mais sobre a segurança da informação e como administrá-la e preservá-la.

2.1 Análise das Perspectivas Atuais sobre Segurança da Informação

O ativo mais valioso para uma organização ou pessoa é a informação. Este grande diferencial competitivo então deve estar disponível apenas para as pessoas de direito. Elaborar e garantir critérios que protejam estas informações contra fraudes, roubos ou vazamentos nas empresas são responsabilidades e habilidades dos gestores e analistas de segurança da informação (SILVA JÚNIOR, 2009).

Um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade.

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Os motivos pelos quais alguém tentaria invadir seu computador são inúmeros como, por exemplo:

- utilizar seu computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor;
- utilizar seu computador para lançar ataques contra outros computadores;
- utilizar seu disco rígido como repositório de dados;
- destruir informações (vandalismo);
- disseminar mensagens alarmantes e falsas;
- ler e enviar *e-mails* em seu nome;
- propagar vírus de computador;
- furtar números de cartões de crédito e senhas bancárias;
- furtar a senha da conta de seu provedor, para acessar a Internet se fazendo passar por você;
- furtar dados do seu computador, como por exemplo, informações do seu Imposto de Renda.

O roubo de informações também pode acontecer com a utilização de celulares. Corporações que dependem de programas gráficos, como as da área de engenharia, estão sujeitas a sofrer com um dispositivo que parece bastante inocente. “Alguém pode abrir o programa, tirar foto da tela do computador e enviá-la para concorrentes”, relata

Menegotto (2011, n.p.). Neste caso, existem softwares que fazem análises no cartão SIM – Subscriber Identity Module – e varrem todas as ações executadas pelo chip. (jordana viotto)

Segundo SILVA JÚNIOR (2009), os principais itens trabalhados num plano de projeto para manutenção e disponibilidade de recursos, sobretudo tecnológicos são:

- Prevenção e detecção de ameaças a rede computacional, também monitoração e controle da rede;
- Definição de políticas e processos de uso de recursos de rede;
- Desativação de recursos e serviços não necessários em servidores e aplicações;
- Ajuste fino de servidores e aplicações (Hardening);
- Cuidados com gerenciamento de identidades e controles de acesso a rede;
- Definição de um plano para aplicação de patches e atualizações no ambiente;
- Definição de um plano de contingência para os recursos e um plano para recuperação de desastres.

Quando se trata de Confidencialidade, vale a pena ressaltar que, as informações devem estar disponíveis apenas a pessoas e/ou outros recursos que tenham direito a elas. Com isso em mente pode-se trabalhar para minimizar ataques a rede computacional da empresa, vazamento de dados através do envio de informações de negócio sem autorização por e-mails, impressões, cópias em dispositivos móveis, também acesso a informações de projetos e departamentos armazenadas em servidores por pessoas não autorizadas. (SILVA JÚNIOR, 2009)

Do mesmo modo ao falar de Integridade deve-se levar em conta que os principais objetivos desta etapa são entender os métodos como processos de negócio são aprovados e repassados, quem são seus proprietários/responsáveis e usuários e buscar ferramentas para monitorar e controlar estas alterações a fim de garantir a integridade.

Portanto, recursos como firewalls, antivírus, criptografia, assinatura digital, backup, processos e outras ferramentas devem ser usadas para garantir o bom funcionamento do ambiente (SILVA JÚNIOR, 2009). Afinal, “destruir informações pode ser surpreendentemente difícil”. (GUTMANN apud FARMER, 2006, p.10)

Levando essa discussão em consideração, fica claro que se tratando de tecnologia e segurança da informação alguns conceitos são fundamentais para sua compreensão. Por este motivo, veja a seguir algumas definições essenciais para essa

compreensão como, por exemplo, os conceitos de *Firewall*, Vírus, *Worm, Trojan*, e, por fim, *Phisinhing.*

3 Análise da atual Concepção de Engenharia Social

O termo **"**engenharia social" (em inglês "*social engineering*") designa a arte de manipular pessoas a fim de contornar dispositivos de segurança, ou seja, obter informações necessárias para conseguir acessar um sistema, roubar dados de bancos ou qualquer outra coisa. Trata-se assim de uma técnica que consiste em obter informações por parte dos utilizadores por telefone, por correio electrônico, por correio tradicional ou contacto directo. A engenharia social é baseada na utilização da força de persuasão e na exploração da ingenuidade dos utilizadores, fazendo-se passar para uma pessoa da casa, um técnico, um administrador, etc. (KIOSKEA, 2010).

Assim, de nada adiantaria um sistema rodar linux, windows, OS/2, Mac OS ou qualquer outro sistema extremamente seguro se no final das contas ele será operado por pessoas, que são sempre sujeitas a falhas ou há más intenções.

Neste último caso as falhas podem ser ocasionadas por hackers, indivíduos que usam a Engenharia Social juntamente a ataques de cunho mais técnico (o que nós tradicionalmente chamamos de chamamos de *hackear*) para obter informações avançadas de bancos e sistemas de segurança. O simples fato de se abrir um arquivo word, ligar um pendrive desconhecido em seu PC ou clicar em um link malicioso já são suficientes para se garantir acesso a um computador. (MITNICK apud PEÇANHA, 2010, n.p.)

O meio mais frequente de combate a essas falhas mostradas são as ferramentas periciais.Mas, para compreendermos as ferramentas periciais, há a necessidade de se conhecer como se dá o processo de exclusão de arquivos do computador**.** Quando apaga-se um arquivo da lixeira ou usa-se SHIFT+DEL, o Windows apenas marca no HD que tal arquivo foi deletado, fazendo o arquivo ficar invisível para o Usuário do sistema. Com isso o arquivo "**deletado**" continua no HD até que um novo arquivo venha ocupar aquele espaço.

Para ficar mais claro, observe a Figura 1. Os blocos em branco representam os espaços vazios no HD. Os vermelhos representam os arquivos gravados em disco:

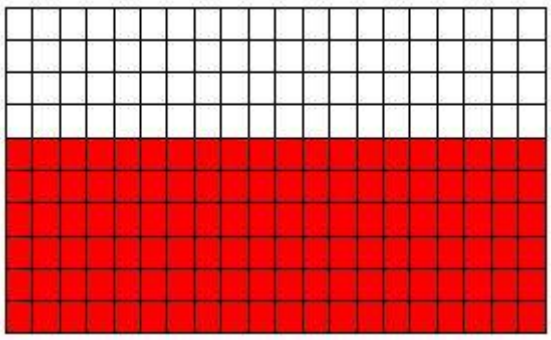

Figura 1: Imagem representativa de arquivos do computador inicialmente. Retirado de: http://recuperaarquivosdeletados.com/

Após alguns arquivos serem deletados, o disco ficaria como segue abaixo (Figura 2); com blocos cinzas representando os arquivos deletados que ainda permanecem no disco e podem ser recuperados por algum programa para recuperar arquivos deletados:

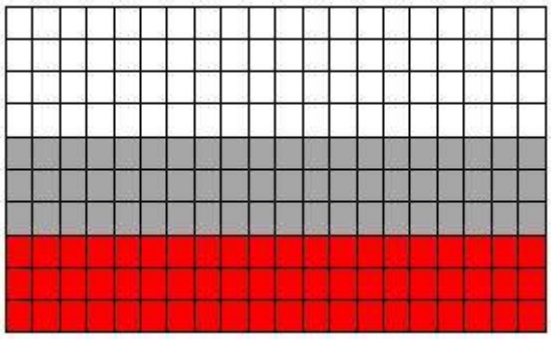

Figura 2: Imagem representativa após algumas exclusões. Retirado de: http://recuperaarquivosdeletados.com/

Se um novo arquivo for gravado no hd, é bem possível que ele seja gravado por cima de algum arquivo deletado. Caso isso aconteça, o arquivo antigo fica sobscrito pelo novo, e parte ou toda informação antiga é perdida.

Compreendido como se dá esse processo de exclusão de arquivos, veja algumas ferramentas periciais na qual esse fato apresentado pode ser utilizado.

4 Esteganografia e Codificação de Huffman

A Esteganografia consiste em ocultar informação de tal forma que sua existência não seja percebida. Ao contrário da criptografia, ela não pode ser detectada.

Arquivos como os de imagem e som possuem áreas de dados que não são usadas ou são pouco significativas. A esteganografia tira proveito disso, trocando essas áreas por informação. O objetivo deste trabalho é criar um programa que utilize arquivos de imagem para ocultar textos (KUNZ, 2010, n.p.).

Kunz (2010) diz ainda que a codificação de Huffman é uma forma de compressão de dados em que representa-se cada um dos caracteres de um texto com códigos binários de comprimento variável. O tamanho do código varia conforme a freqüência com que ocorre no texto, atribuindo-se códigos menores aos caracteres mais freqüentes e maiores aos menos freqüentes.

Para o examinador, é imperativo que se conheçam formatos de imagens para avaliar o tamanho em disco de um arquivo. Muitas técnicas de ocultação de mensagens aumentam consideravelmente o tamanho do arquivo. Imagens podem possuir variações de cores e aumento significativo da granularidade. (BUSTAMANTE, 2010, n.p.)

Na figura 3 pode-se observar uma imagem com uma mensagem escondida utilizando a técnica da esteganografia.

Figura 3: Imagem com mensagem camuflada utilizando esteganografia: Retirado de: http://www.webturotiais.org/esteganografia-a-arte-de-esconder/

Sabendo-se que uma imagem é formada por 3 canais de cores (R,G,B) de 8 bits cada um, basta alterar o bit menos significativo, não ocorrendo mudanças perceptíveis na imagem. Assim é possivel camuflar em uma imagem um texto usando apenas o bit menos significativo de cada canal. KUNZ (2010) diz que a steganografia é implementada em uma imagem da seguinde forma;

> Inicialmente o programa lê o texto e calcula a freqüência com que cada um dos caracteres aparece. Assume-se que cada um é uma árvore de um nodo apenas. Pesquisa-se, então, os dois com menor freqüência e combina-os para formar uma árvore. A freqüência dos dois é somada e atribuída à raiz. Repete-se esta etapa até que haja uma única árvore. No final, tem-se uma árvore com os caracteres do texto na folhas. Para se ter o código de cada um basta convencionar para um nodo qualquer 0 se for um filho à esquerda e 1 à direita. O código do dígito será o caminho percorrido da raiz até a folha. (KUNZ, 2010, n.p.).

Figura 4: Etapas da codificação de Huffman. Retirado de Kunz (2010, n.p.)

Para que a decodificação pode ser realizada é necessário incluir a árvore. Por isso, no início da seqüência de bits do arquivo de imagem, é gravada a lista de caracteres da árvore em percorrimento pré-ordem. No exemplo acima, tem-se: @@a@bdc .

Na parte inicial do arquivo de imagem é gravada a string da árvore em binário seguida de um caractere especial que indica o fim da árvore e o início da seqüência codificada. Antes da codificação do texto, é acrescentado um outro caractere especial que indica o fim da frase. Ele é incluído na árvore assim como os outros caracteres mais terá a função de indicar para o programa o fim da frase e conseqüentemente o fim da leitura dos bits da imagem na decodificação. (KUNZ, 2010).

4.1 Lsb

Uma das técnicas de esconder informações em imagens JPEG, usando o ruído, é conhecida como LSB (Least Significant Bits). Ela consiste em usar os bits menos significativos para guardar os dados que se deseja camuflar. Em uma imagem JPEG, trocar os bits menos significativos pode mudar a intensidade de um pixel em no máximo 1%. Isto faz com que a técnica seja uma ótima solução esteganográfica, uma vez que a imagem fica praticamente inalterada, principalmente no que diz respeito à percepção visual do ser humano (WAYNER 2002 apud UFRJ, 2010, n.p.)

5 SOFTWARES RELACIONADOS

Neste capítulo será abordado a definição e funcionamento de softwares ligados a pericia forense computacional e crimes digitais, estes softwares podem ser tanto relacionados a segurança da informação quanto a recuperação de dados e também localização de usuários.

5.1 Firewall: definição e propriedades

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

Assim, a razões para utilizar firewall podem ser elencadas:

> 1 - o firewall pode ser usado para ajudar a impedir que sua rede ou seu computador seja acessado sem autorização. Assim, é possível evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers;
> 2 - o firewall é um grande aliado no combate a vírus e cavalos-de-tróia, uma vez que é capaz de bloquear portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados;
> 3 - em redes corporativas, é possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo descobrir quais usuários as efetuaram. (ALECRIM, 2010, n.p.)

5.2 A compreensão de Vírus, Worms e Trojan

Referente à tecnologia, um vírus é um código de computador que se anexa a um programa ou arquivo para poder se espalhar entre os computadores, infectando-os à medida que se desloca. Ele infecta enquanto se desloca. Os vírus podem danificar seu software, hardware e arquivos.

Para Microsoft, o vírus pode ser caracterizado por um:

> Código escrito com a intenção explícita de se auto duplicar. Um vírus tenta se alastrar de computador para computador se incorporando a um programa hospedeiro. Ele pode danificar hardware, software ou informações (MICROSOFT, 2010, n.p.).

Já um Worm (minhoca, em português), verme em computação, é um programa auto-replicante, semelhante a um vírus. Entretanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, já o Worm é um programa

completo e não precisa de outro programa para se propagar. Um worm pode ser projetado para tomar ações maliciosas após infestar um sistema, além de se auto-replicar, tais como: deletar arquivos em um sistema ou enviar documentos por email. Daí, o worm pode tornar o computador infectado vulnerável a outros ataques e provocar danos apenas com o tráfego de rede gerado pela sua reprodução – o Mydoom, por exemplo, causou uma lentidão generalizada na Internet no pico de seu ataque.

Enfim, assim como o mitológico cavalo de Tróia parecia ser um presente, mas na verdade escondia soldados gregos em seu interior que tomaram a cidade de Tróia, os cavalo de Tróia da atualidade são programas de computador que parecem ser úteis, mas na verdade comprometem a sua segurança e causam muitos danos. Um cavalo de Tróia recente apresentava-se como um email com anexos de supostas atualizações de segurança da Microsoft, mas na verdade era um vírus que tentava desativar programas antivírus e firewalls.

> Cavalo de Tróia (s. m.) Um programa de computador que parece ser útil, mas na verdade causa danos. (MICROSOFT, 2010, n.p.)

5.3 A compreensão de Phishing

O primeiro uso documentado da palavra "phishing" se deu em 1996. Muitas pessoas acreditam que se originou como uma ortografia alternativa para "fishing", "pescaria" em inglês, como em "pescar informações" (WILSON, 2010, n.p.).

Phishing é um tipo de fraude projetada para roubar seus valiosos dados pessoais, como números de cartões de crédito, Windows Live IDs, senhas e dados de outras contas, entre outras informações.

Segundo MICROSOFT (2008), você pode encontrar tentativas de phishing nas seguintes formas:

- Em emails, mesmo quando eles parecem vir de um colega ou de alguém conhecido.
- No seu site de relacionamento social.
- Em um site falsificado que aceite doações para caridade.
- Em sites que falsificam sites que lhe são familiares usando endereços da Web ligeiramente diferentes, na esperança de que você não perceba a diferença.
- Em seu programa de mensagens instantâneas.
- No celular ou em outro dispositivo móvel. (MICROSOFT, 2008, n.p.)

Veja na figura abaixo (Figura 4) um exemplo do reporte dessa atividade:

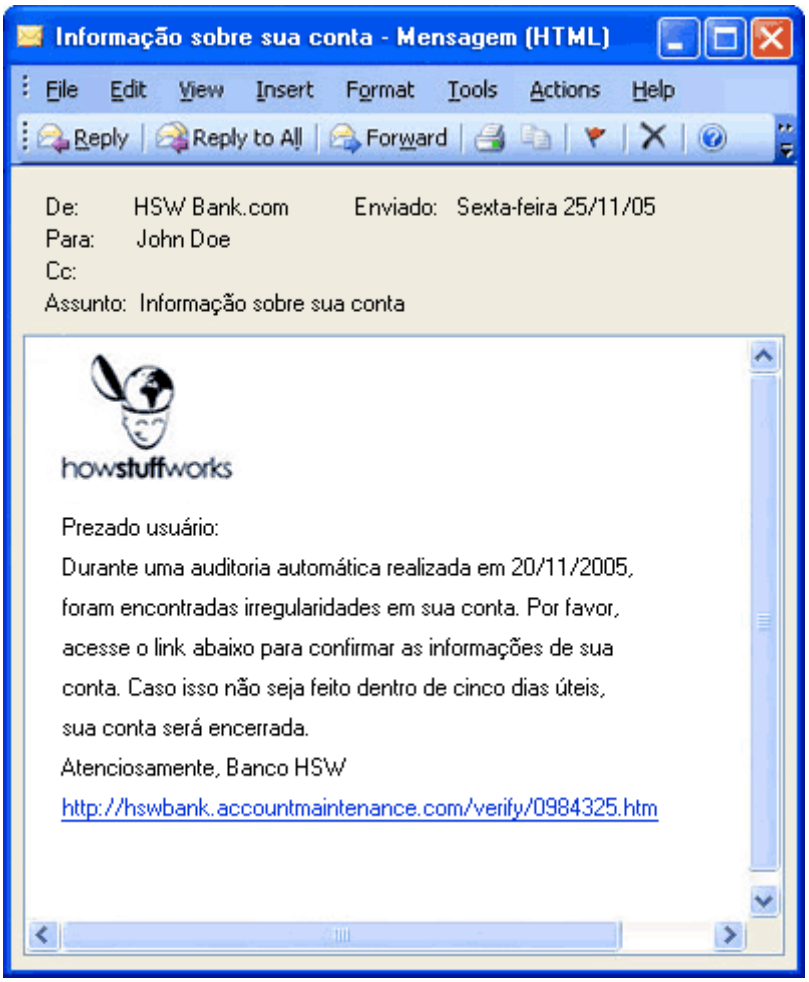

Figura 5: Reporte de Pishing em programa. Retirado de http://informatica.hsw.uol.com.br/phishing.htm

Para identificar um Phishing, veja o roteiro proposto por SYMANTEC (2007, n.p.):

> "Os criadores do phishing fazem-se passar por empresas legítimas e usam o e-mail para solicitar informações pessoais e direcionar os destinatários a fornecê-las em websites maliciosos.
> Eles tendem a usar linguagem emocional, como táticas de intimidação ou solicitações urgentes, para induzir o destinatário a fornecer tais informações
> Os sites de phishing podem ter a mesma aparência dos sites legítimos, pois costumam usar imagens com direitos autorais desses sites legítimos.
> As solicitações por informações confidenciais através de e-mail ou de mensagens instantâneas não são normalmente legítimas.
> Em geral, as mensagens fraudulentas não são personalizadas e podem ter propriedades semelhantes, como detalhes no cabeçalho e no rodapé."

5.4 PCI

O PCI é um programa gratuito e bem eficiente para **recuperação de dados**. Ele suporta os sistemas **FAT 12/16/32 e NTFS**. e permite recuperação de arquivos em **HDs, Disquetes, Pen drives etc. (**PCI, 2010, n.p.)

5.5 Recover My Files

O Recover My Files é um software de recuperação de dados de computador. Irá recuperar ficheiros que tenham sido eliminados e removidos (ou eliminados sem imediatamente) da Reciclagem do Windows.

Trata-se de um software de recuperação de dados de computador. Irá recuperar ficheiros que tenham sido eliminados e removidos (ou eliminados sem imediatamente) da Reciclagem do Windows.

Este programa irá encontrar qualquer tipo de ficheiro eliminado, mas também irá procurar especificamente ficheiros que você tenha designado. O Recover My Files também irá detectar unidades corrompidas, que o Windows já não reconhece, formatadas e até discos que tenham sido formatados e nos quais tenha sido instalado um novo Sistema Operativo.

Para tal, o Recover My Files (figura 5) não modifica o conteúdo da unidade que está a ser pesquisada, por isso, pode realizar a recuperação de dados em segurança (GETDATA, 2010, n.p.).

Figura 6: Recover My Files. Retirado de Getdata (2010, n.p.).

5.6 EnCase

O EnCase é um sistema integrado de análise forense baseado no ambiente Windows. Ele é muito utilizado por oficiais da lei e profissionais da segurança de computadores em todo o mundo. O processo utilizado pelo EnCase começa com a criação das imagens dos discos (disquetes, Zips, Jaz, CD-ROMs e discos rígidos) relacionados ao caso investigado. Depois da criação das imagens, chamadas de EnCase Evidence Files, pode-se adicioná-las a um único caso (case file) e conduzir a análise em

todas elas simultaneamente. O ambiente Windows não é considerado apropriado por muitos profissionais da área para a prática forense, uma vez que ele rotineiramente altera os dados e escreve no disco rígido sempre que é acessado. Mas, o EnCase não opera na mídia original ou discos espelhados, ele monta os Evidence Files como discos virtuais protegidos contra escritas. Então, o EnCase (não o sistema operacional) reconstrói o sistema de arquivos contido em cada Evidence File, permitindo ao investigador visualizar, ordenar e analisar os dados, através de uma interface gráfica. (HOLPERIN; LEOBONS, 2011, n.p.).

5.7 Smart whois

O Smart whois (Figura 6) é uma aplicação de escritório para arrecadar informações sobre os domínios de Internet ou as IP, como os titulares, as empresas onde se hospedam os domínios, os países de procedência, etc.

Quando se faz uma busca, oferece a informação do servidor onde está hospedado o domínio e da empresa titular do servidor, ou seja, a empresa que oferece hospedagem ao domínio. Também permite conhecer a rede ou o centro de dados onde está incluída a empresa de hospedagem. Tudo isso, com dados das empresas, seu serviço técnico, etc.

Também pode ser realizado um típico whois para extrair a informação dos titulares de um domínio e seus dados de contato.

A aplicação está preparada para arrecadar informação, de forma transparente para o usuário, de mais de 60 servidores do mundo, o que permite extrair os dados de qualquer domínio de um lugar ou outro.

Também têm opções de exportação dos dados obtidos a HTML, texto, XML e outros formatos, para salvar a informação das buscas e utiliza-la em outros programas ou banco de dados.

A interface é simples e a apresentação de dados, além de completa, é muito limpa (SMARTWHOIS, 2010, n.p.).

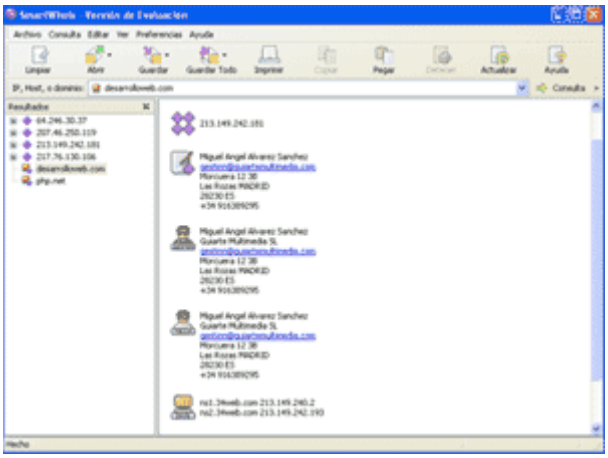

Figura 7: SMARTWHOIS. Retirado de SmartWhois (2010, n.p.).

5.8 e-mailTracker:

O programa conhecido como emailTracker fornece o local de origem do e-mail, sua rota e a empresa responsável. (Figura 7)

Figura 8: EmailTracker. Retirado de Vargas (2010, n.p.)

6 METODOLOGIA

Definidas como “estado da arte” ou “estado do conhecimento”, estes tipos de pesquisas de caráter bibliográfico visam mapear e discutir uma certa produção acadêmica em diferentes campos do conhecimento (FERREIRA, 2002).

Para Dencker (2002), o início da pesquisa é marcado pela pesquisa bibliográfica por meio de livros, monografias, teses de mestrado e/ou doutorado, e da internet. Através de trabalhos que se adequam ao tema em estudo, a pesquisa se torna mais contundente e rica, pois são diversas opiniões e teorias que entram em conflito para se obter uma idéia em comum.

Ao observar as diferentes técnicas utilizadas na pericia forense computacional pode-se perceber sua vasta gama de elementos.

Existem diversificadas técnicas a ser utilizadas pelos peritos, possuindo sempre diversos programas em cada uma destas tecnicas.

Pode-se observar que o sistema operacional utilizado pelo infrator influencia na sua eficacia em se esconder das autoridades, mas nenhum criminoso virtual age sem deixar vestigios. Do lado do perito o sistema operacional mostra-se ainda mais importante, pois alguns sistemas costumam sobrescrever arquivos, apagando assim dados que eram desejados na coleta de provas.

Foi possivel observar também, que mesmo um usuário utilizando um e-mail anônimo, pode ser localizado, a maior dificuldade neste tipo de crime seria o infrator que utiliza-se de computadores publicos, como os de lan house para cometer os delitos. Para combater estes problemas varios estados tem criado leis para tornar obrigatorio o cadastro de usuarios das lan houses, mas nem sempre esta pratica é realizada e nem todos os lugares possuem esta lei, pois não se trata de uma lei federal.

6.1 Resultados Obtidos

Quanto à legislação, pode-se verificar que as leis atuais possuem total capacidade para julgar quaisquer das atuais ameaças e crimes conhecidos até o momento, vale ressaltar que para isto o Brasil utiliza-se da legislação do mundo “real”, pois apesar de certos crimes do mundo “virtual” possuir alguns aspectos diferentes, sua essência continua a mesma.

Sobre os sistemas de firewall atuais, os sistemas comercias mostram-se ferramentas complementais na segurança de um sistema, pois estes, mesmo os sistemas

comerciais mais caros possuem vunerabilidades, quanto aos firewalls de uso doméstico, são muito ineficientes para um infrator bem instruido técnicamente.

Virus, worms, trojans e outros programas que visam criar vunerabilidades nos sistemas são um grande problema para a segurança, a única maneira de evitalos totalmente é com um sistema totalmente isolado de conexões externas, incluindo a utilização de dispositivos móveis de dados, sendo assim a única maneira de evita-los em outro tipo de sistema, é a prevenção, seja tentando prever os virus que serão lançados, encontrando as vunerabilidades antes dos criminosos, ou agindo rapidamente quando estes forem localizados.

Nas técnicas de phishing, foi possivel verificar que a melhor maneira de evitalos é um usuário bem instruído, entretanto, algumas novas tecnologias vêm provando ser um bom auxílio quando o assunto é evitar ser enganado por falsas mensagens, porém a ação final ainda depende totalemente do usuário, pois este decide o acesso ao link ou não.

Os softwares de recuperação de dados hoje existentes, são muito eficientes, mesmo utilizandos diversas técnicas diferentes, como a formatação repetitiva do hard disk, uma pessoa pode ter muita dificuldade para eliminar os dados contidos nestes dispositivos, entretanto uma falha pode ter sido fornecida pelos próprios peritos.

A possivel falha torna-se aparente, por um simples fato, peritos usam sistemas operacionais especificos para recuperação de dados, pois sistemas como windows podem sobrescrever os arquivos. Então utilizando esta lógica, caso uma pessoa queira desaparecer com os arquivos do seu hard disk, não deveria utilizar técnicas como formatar diversas vezes, apenas formatar uma vez e sobrescrever todo o disco com informações inúteis, após isto, formatar novamente, acredito que este pode ser um método mais eficaz.

Quanto aos softwares de localização de usuários, na teoria são muito eficientes, pois podem localizar um computador facilmente, o problema seria o criminoso utilizar um computador publico que não mantem registro de seus usuários, assim sua localização estaria afetada.

Engenharia social, uma maneira muito eficiente de se tornar um criminoso virtual, não necessita conhecimentos computacionais avançados para realiza-lo, mas é claro que o conhecimento na área ajuda a ampliar o leque de oportunidades.

Esteganografia, um método que pode ser utilizado para esconder mensagens ou informações sem nunca ser detectado, talvez a melhor maneira atual de esconder dados, muito eficiente, praticamente imperceptível, e além de tudo, simples.

7 CONSIDERAÇÕES FINAIS

Entende-se que o objetivo foi atingido, pois deu-se como objetivo desta investigação ao esclarecer do que se trata a pericia forense, de onde são obtidas as provas e como obtê-las, para que sejam apresentadas de maneira confiável em um processo judicial; e demonstrar quais são os crimes digitais, qual o papel do perito computacional, mostrar as técnicas utilizadas pelos criminosos na obtenção de acesso a dados privados, assim como as técnicas utilizadas para solucionar os crimes e recuperar dados quando estes forem danificados.

Foi mostrado o quão dificil pode ser encontrar um criminoso virtual, pois este pode utilizar de diversos artificios para se comunicar, para esconder programas maliciosos, ou na tentativa de esconder sua localização. Mas também se mostrou que é muito mais difícil um criminoso esconder-se para sempre do que um perito localiza-lo, pois o criminoso sempre na sensação de segurança e anonimato da internet acaba deixando um vestigio que leva a sua localização.

Deve-se salientar, no entanto, a necessidade de mais estudos na área devido à importância de tal tecnologia, pois devido a crescimento constante da internet, dos mercados envolvidos na tecnologia, a tendencia é que este mundo, o virtual, esteja cada vez mais repleto de usuários, tanto os usuários corretos, quanto os usuários que agem de forma criminosa.

Vale ressaltar que os criminosos sempre encontraram novas maneiras de burlar a segurança virtual, e que estas brechas sempre existirão, e que cabe aos peritos em segurança computacional a criação de sistemas mais seguros, e ao perito forense, encontrar os criminosos e as provas necessarias para que estes nao continuem cometendo seus atos criminosos.

BIBLIOGRAFIA REFERÊNCIAS

ALECRIM, Emerson. **Firewall: conceitos e tipos.** Disponível em: < http://www.infowester.com/firewall.php > Acesso em: 10 mai 2010.

BARROS, Eduardo Gomes. **Elementos Básicos de Perícia Forense Computacional.** Disponível em < http://www.mpm.gov.br/pagina-inicial/mpm/servicos/assessoria-de-comunicacao/anexos/perícia_forense_computacional_conceitos.pdf > Acesso em: 3 mai 2010.

BUSTAMANTE, Leonardo. **Esteganografia** - A Arte de Esconder. Disponível em: <http://imasters.uol.com.br/artigo/4500/forense/esteganografia_a_arte_de_esconder/> Acesso em: 1 jun 2010.

BUSTAMANTE, Leonardo. **Perícia Forense Computacional em Sistemas de Arquivos.** Disponível em: <http://www.tecdom.com.br/blog/2008/07/05/perícia-forense-computacional-em-sistemas-de-arquivos-a-monografia/> Acesso em: 3 mai 2010.

CANSIAN, Adriano. **Conceitos Para Perícia Forense Computacional**. Monografia(Depto. De Ciência da Computação e Estatística) UNESP, São José do Rio Preto.

CERT. BR . **Cartilha de Segurança Para Internet.** Disponível em: < http://cartilha.cert.br/conceitos/> Acesso em: 9 mai 2010.

DINAMARCO, Cândido Rangel. **Instituições de Direito Processual Civil**. São Paulo, Malheiros, 2001. v. III, p. 584.

DE PAULA, Alexandre Sturion**. Epítome da prova pericial no estatuto processual civil brasileiro.** Disponível em: < http://www.uj.com.br/publicacoes/doutrinas/?action=doutrina&iddoutrina=1266 > Acesso em: 6 mai 2010.

DENCKER, Ada de Freitas Maneti. **Pesquisa e interdisciplinaridade no Ensino Superior**: uma experiência no Curso de Turismo. São Paulo: Aleph, 2002. 111p.

ELIAS, Paulo. **Legislação Específica de Direito da Informática.** Disponível em: <http://www.direitodainformatica.com.br/?page_id=33> Acesso em: 20 abr 2010.

FERREIRA, N. S. A. AS PESQUISAS DENOMINADAS "ESTADO DA ARTE". In: **Educação & Sociedade,** ano XXIII, no 79, Agosto/2002

GETDATA. **Recover My Files**. Disponível em: <http://www.recovermyfiles.com/pt/guia-iniciacao-rapida.php> Acesso em: 6 mai 2010.

HOLPERIN, Marco; LEOBONS, Rodrigo. **ANÁLISE FORENSE.** Disponível em:

< http://www.gta.ufrj.br/grad/07_1/forense/> Acesso em: 20 mai 2010.

KIOSKEA. **Engenharia Social**. Disponível em: <http://pt.kioskea.net/contents/attaques/ingenierie-sociale.php3> Acesso em: 12 mai 2010.

KUNZ, Leonardo. **ESTEGANOGRAFIA EM IMAGENS USANDO CODIFICAÇÃO DE HUFFMAN**. Disponível em: < http://www.inf.ufrgs.br/~lkunz/cpd/> Acesso em: 1 jun 2010.

MICROSOFT. **RECONHEÇA TENTATIVAS DE PHISHING E EMAIL FRAUDULENTOS.** Disponível em: < http://www.microsoft.com/brasil/protect/yourself/phishing/identify.mspx> Acesso em: 10 mai 2010.

MICROSOFT. **O Que são Vírus, Worms e Cavalos de Tróia?.** Disponível em < http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx#EXC> Acesso em: 12 mai 2010.

PEÇANHA. **Kevin Mitnick explica o que é Engenharia Social .** Disponível em < http://www.fayerwayer.com.br/?tag=kevin-mitnick > Acesso em: 12 mai 2010.

PIMENTA, Flávio. **Perícia forense computacional baseada em sistema operacional Windows XP Professional.** Disponível em: < http://www.datasecur.com.br/academico/ForenseXP.pdf > Acesso em: 10 mai 2010.

POPPER, Marcos; BRIGNOLI, Juliano. **ENGENHARIA SOCIAL:** Um Perigo Eminente**.** Disponível em: < http://fabricio.unis.edu.br/SI/Eng_Social.pdf > Acesso em: 7 mai 2010.

SILVA, Marcos Vinicius. **O Que é Segurança da Informação.** Disponível em: < http://webinsider.uol.com.br/2009/09/23/o-que-e-seguranca-da-informacao/> Acesso em: 15 mai 2010.

SYMANTEC. **COMO ELES ATACAM –** Phishing. Disponível em: < http://www.symantec.com/pt/br/norton/security_response/phishing.jsp> Acesso em: 10 mai 2010.

THEODORO JÚNIOR, Humberto. **Curso de Direito Processual Civil**. 40ª edição, São Paulo: Forense, 2003;

TIROTTI, Robson. **PERÍCIAS EM MEIOS ELETRÔNICOS**: Maximizando o Valor da Prova**.** Monografia(Direito Eletrônico e Tecnologia da Informação) UNIGRAN, Dourados, 2008.

TOSCANO, Wagner. **Auditoria Forense Computacional** – Introdução**.** Disponível em: < http://wagnertoscano.eti.br/Pool/%5BAUF%5DIntroducao.pdf> Acesso em: 9 mai 2010.

TREVENZOLI, Ana Cristina. **Perícia Forense Computacional** – Ataques, Identificação da Autoria, Leis e Medidas Preventivas. Disponivel em < http://www.datasecur.com.br/academico/Perícia_Forense_Computacional_ataques.pdf > Acesso em: 2 mai 2010.

UFRJ. **Esteganografia**. Disponível em:

< http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html#historia

> Acesso em: 10 dez 2010.

VARGAS, Raffael. **Perícia Forense Computacional** - Ferramentas Periciais. Disponível em: <http://imasters.uol.com.br/artigo/6485/forense/perícia_forense_computacional_ferramentas_periciais/ > Acesso em: 27 fev 2010.

VIOTTO, Jordana. **Quem são e Como Trabalham os Peritos em Forense Computacional.** Disponível em: < http://www.itweb.com.br/noticias/index.asp?cod=20800 > Acesso em: 17 mai 2010.

WILSON, Tracy. **Como Funciona o Phishing.** Disponível em: <http://informatica.hsw.uol.com.br/phishing.htm> Acesso em: 12 mais 2010.

ANEXO A

Legislação Específica de Direito da Informática

Lei 9.610/98 – Dir. Autorais
Dec. 4.533/2002 Conv. de Berna | PCP
AND/AV - Lei nº 10.695/2003
Lei 9.609/98 – Programa de Computador
Dec.2556/98
Lei 9.279/96 – Prop. Industrial | (detalhes)
Alt.Lei 10.196/2001 – Convenção de Paris
MP 2.200-2/2001 – ICP BRASIL (detalhes)
(cf. art. 10)
Lei 9.800/99 – Atos Proc. – Sist. Transmissão
Lei 9983/2000 – Altera o CP – Sist. Inform.
(cf. arts. 313-A; 313-b)
Lei 10.259/2001 – Juizados Especiais
(cf. Arts. 8 e 14)
UNCITRAL – Lei Modelo 1996 (Com. Eletr.)
2001 – Ass. Eletrônicas / Contratos Intern.
Projeto nº 4.906/2001 (PLS nº 672/99)
Comércio Eletrônico
Projeto nº 84/1999 – Crimes Inf./Internet
Decreto nº 5.450/2005 – Pregão Eletrônico
Lei nº 11.101/2005 – Falências
(cf. arts. 168, § 1º, inc. III e 196)
AC-JUS/Res. Conj. STJ/CJF nº 001/2004
Lei nº11.196/2005-REPES/RECAP/PID/IF-IT
Lei nº 11.280, de 16.2.2006

Decreto nº 6.605, de 14/10/2008 – Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva – COTEC.

Lei nº 11.341/2006 – Altera o parágrafo único do art. 541 do Código de Processo Civil – Lei nº 5.869, de 11 de janeiro de 1973, para admitir as decisões disponíveis em mídia eletrônica, inclusive na Internet, entre as suscetíveis de prova de divergência jurisprudencial.

LEI Nº 11.382/2006 – Altera dispositivos da Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil, relativos ao processo de execução e a outros assuntos.

LEI Nº 11.419/2006 – Dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.

DECRETO Nº 6.022/2007 – Institui o Sistema Público de Escrituração Digital – Sped.

Resolução STJ nº 2, de 24/04/2007 – Dispõe sobre o recebimento de Petição Eletrônica no âmbito do Superior Tribunal de Justiça.

Resolução STJ nº 9, de 05/11/2007- Altera o art. 1º da Resolução nº 2, de 24 de abril de 2007, que dispõe sobre o recebimento de Petição Eletrônica no âmbito do Superior Tribunal de Justiça.

Resolução STF nº 344, de 25/05/2007 – Regulamenta o meio eletrônico de tramitação de processos judiciais, comunicação de atos e transmissão de peças processuais no Supremo Tribunal Federal (e-STF) e dá outras providências.

Portaria STF nº 73, de 30/05/2007 – Estabelece normas complementares para a tramitação do processo eletrônico no Supremo Tribunal Federal.

Instrução Normativa TST nº 30, de 13/09/2007 – Regulamenta, no âmbito da Justiça do Trabalho, a Lei n° 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.

Resolução STJ nº 8, de 20/09/2007 – Institui o Diário da Justiça Eletrônico do Superior Tribunal de Justiça – DJ on-line e dá outras providências.

Resolução STJ nº 11, de 11/12/2007 – Altera o art. 5º da Resolução n. 8, de 20 de setembro de 2007, que institui o Diário da Justiça Eletrônico do Superior Tribunal de Justiça – DJ on-line.

Resolução STF nº 350, de 29/11/2007 – Dispõe sobre o recebimento de Petição Eletrônica com Certificação Digital no âmbito do Supremo Tribunal Federal e dá outras providências.