PERÍCIA FORENSE COMPUTACIONAL: análise de fraudes, ataques e invasões, leis, entidades, identificação da autoria e medidas preventivas

Krenak Marques Canedo Júnior [*]
Marta Alves de Souza [**]
Ulisses Procópio Pascoal Tôrres[***]

RESUMO

Devido ao aumento da utilização de computadores e da Internet nos últimos anos, tornou-se essencial a apuração dos crimes realizados através de ambientes computacionais. Para a investigação e coleta de evidências destes crimes por meio de computadores surgiu a Perícia Forense Computacional. A proteção de dados tornou-se necessária, pois os ataques feitos por criminosos na Internet e nos computadores provocam danos, por vezes, imensuráveis para todos os usuários, sejam pessoas físicas, governo ou empresas. Este estudo tem como objetivo descrever os principais conceitos e ferramentas utilizadas pela perícia forense computacional, para auxiliar na coleta, manutenção e análise de evidências digitais para promover a reconstituição dos eventos encontrados. Justifica-se este estudo pelo crescimento das investigações criminais, cujas principais evidências estão armazenadas em formato digital e para auxiliar os usuários a conhecerem as ameaças no ambiente Internet. Pode-se constatar que os estudos sobre a área favoreceu a prevenção e proteção das informações, que a falta de padronização e a ausência de normas pode possibilitar erros para evidências despercebidas e que não existe um computador ou dispositivo totalmente seguro, fazendo com que a forense computacional seja necessária.

Palavras-chaves: Forense computacional. Fraudes eletrônicas. Segurança na Internet.

ABSTRACT

Because the increased use of computers and the Internet in recent years, it became essential to the calculation of the crimes carried out by computing environments. For the investigation and evidence collecting of crimes by means of computers came the Computer Forensics. Data protection has become necessary because attacks by criminals on the Internet and computers to cause harm, sometimes immeasurable for all users, whether individuals, companies or government. This study aims to describe the main concepts and tools used by computer forensic expertise to assist in the collection, maintenance and analysis of digital evidence to promote the reconstruction of events found. This study is justified by the growth of criminal investigations, the main evidence is stored in digital format and to help users to know the threats in the Internet environment. It is evident that studies of the area favors the prevention and protection of information, lack of standardization and lack of standards can allow for errors and overlooked evidence that there is not a completely secure computer or device, causing the forensic computer is necessary.

Key-words*:* Computer forensics. Eletronic fraud. Internet security.

[*] Analista de TI – Analista de TI das empresas Solução/Imac, krenakj@hotmail.com.
[**] Mestre em Administração e planejamento de sistemas de informação (PUCCAMP), e-mail: profamarta.souza@gmail.com
[***] Mestre em Engenharia da produção (UFSC), e-mail: ulisses@uai.com.br.

1 INTRODUÇÃO

O crime eletrônico diferencia-se dos crimes tradicionais em função do seu modo de operação, pois envolve a utilização de dispositivos eletrônicos, de computadores e da Internet para a execução de ação ou omissão, típica, antijurídica e culpável. Entretanto, os autores dos atos ilícitos convencionais – aqueles cometidos sem o uso de computadores – os responsáveis por crimes virtuais devem ser identificados, julgados e penalizados. No entanto, essa é uma tarefa complexa devido à possibilidade de anonimato dos criminosos e diante do fato de que as evidências do crime podem estar distribuídas em diversos servidores espalhados pela Internet, possivelmente em computadores localizados em regiões distantes daquelas onde as vítimas se encontram (PEREIRA, 2007).

Entre as ocorrências mais comuns das fraudes eletrônicas encontram-se a calúnia, difamação e injúria via e-mail, o roubo de informações confidenciais e a remoção de arquivos. Além disso, crimes como pedofilia, fraudes e o tráfico de drogas via Internet também são atos ilícitos constantemente realizados com o apoio de computadores (DATA SECYRITY, 2008).

As fraudes eletrônicas representam, atualmente, uma grande ameaça tanto às grandes, médias e pequenas empresas, quanto às pessoas físicas. O crescimento do comércio eletrônico tem gerado facilidade, agilidade e velocidade nas transações comerciais e financeiras cotidianas, mas sua segurança ainda é questionável.

O problema deste estudo tem como base a segurança na Internet e levanta as seguintes questões: Existe necessidade da disciplina Forense computacional? Os estudos sobre este tema favorecem a investigação, a prevenção e proteção das informações?

Este estudo tem como objetivo geral analisar os principais conceitos e ferramentas utilizadas pela perícia forense computacional, para auxiliar na coleta, manutenção e análise de evidências digitais para promover a reconstituição dos eventos encontrados. Os objetivos específicos são apresentar conceitos e noções de forense computacional e descrever ferramentas aplicadas na forense computacional.

Forense Computacional pode ser definida como a inspeção científica e sistemática em ambientes computacionais, com a finalidade de angariar evidências derivadas de fontes digitais, tendo como objetivo, promover a reconstituição dos eventos encontrados.

Este estudo trata da forense computacional, um tema que tem recebido atenção tanto da comunidade científica quanto da indústria. No âmbito acadêmico, o interesse deve-se ao pouco conhecimento sobre o tema e de vulnerabilidades a qual estão expostos os usuários frente as ameaças cada vez mais sofisticadas e poderosas dos criminosos. No contexto da indústria, este interesse justifica-se pela grande quantidade de investigações criminais, cujas principais evidências estão armazenadas em formato digital.

2 REFERENCIAL TEÓRICO

2.1 Forence Computacional

Forence Computacional é o ramo da criminalística que compreende a aquisição, preservação, restauração e análise de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais (NOBLETT; POLLITT; PRESLEY, 2000).

Uma perícia em um computador suspeito de invasão ou mesmo em um computador apreendido em alguma batida policial envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise (OLIVEIRA, 2002). Ao contrário das outras disciplinas forenses, que produzem resultados interpretativos, a forense computacional pode produzir informações diretas, que por sua vez, são decisivas no caso investigado (NOBLETT; POLLITT; PRESLEY, 2000).

2.2 Perícia Forense

Perícia Forense Aplicada as Redes é o processo de coleta, recuperação, análise e correlacionamento de dados que visa, dentro do possível, reconstruir o curso das ações e recriar cenários completos e fidedignos. No Manual de Patologia Forense do Colégio de Patologistas Americanos (1990), a ciência forense é definida como “a aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de

comportamento social para que não se cometam injustiças contra qualquer membro da sociedade". Então, pode-se definir a perícia forense aplicada a redes como o estudo do tráfego de rede para procurar a verdade em questões cíveis, criminais e administrativas para proteger usuários e recursos de exploração, invasão de privacidade e qualquer outro crime promovido pela contínua expansão das conexões em rede (FREITAS, 2003).

Análise Pericial - A análise pericial é o processo usado pelo investigador para descobrir informações valiosas, a busca e a extração de dados relevantes para uma investigação, que pode ser dividido em duas partes: análise física e análise lógica (FREITAS, 2003).

A análise física é a pesquisa de seqüências e a extração de dados de toda a imagem pericial, dos arquivos normais às partes inacessíveis da mídia. Nesta análise são investigados os dados brutos da mídia de armazenamento. Eventualmente, pode-se iniciar a investigação por essa etapa, por exemplo, quando investiga-se o conteúdo de um disco rígido desconhecido ou danificado. Após o software de criação de imagens fixar as provas do sistema, os dados podem ser analisados por três processos: uma pesquisa de seqüência, um processo de busca e extração e uma extração de espaço subaproveitado e livre de arquivos. Todas as operações são realizadas na imagem pericial ou na cópia restaurada das provas (FREITAS, 2003).

A análise lógica consiste em analisar os arquivos das partições do disco rígido. O sistema de arquivos é investigado no formato nativo, percorrendo-se a árvore de diretórios do mesmo modo que se faz em um computador comum. Durante um exame de arquivos lógicos, o conteúdo de cada partição é pesquiso utilizando um sistema operacional que compreenda o sistema de arquivos. Neste estágio ocorre a maior parte dos erros de manipulação das provas. O investigador precisa estar ciente de todas as medidas tomadas na imagem restaurada. É por isto que quase nunca se usa diretamente sistemas operacionais mais convenientes, como o Windows 95/98/NT/2000/XP. Novamente, o objetivo básico é proteger as provas contra alterações. Montar ou acessar a imagem restaurada a partir de um sistema operacional que entenda nativamente o formato do sistema de arquivos é muito arriscado, pois normalmente o processo de montagem não é documentado, não está à disposição do público e não pode ser verificado. A imagem restaurada precisa ser protegida, por isso é que cada partição é montada no sistema Linux, em modo somente leitura. O sistema de arquivos montado é, então, exportado por meio do servidor de arquivos Samba para a rede segura do laboratório, onde o sistema Windows 2000, carregado com visualizadores de arquivos, pode examinar os

arquivos. Considera-se que a abordagem é ditada pelo próprio caso. Se fizer uma duplicata pericial de um sistema Irix 6.5, é provável não ser necessário utilizar o Windows 2000 para visualizar os dados (FREITAS, 2003).

2.3 Privacidade

Para realizar uma análise forense em uma máquina que trabalha como um servidor de serviços tais como servidor de email, servidor de arquivos, servidor de usuário é necessário tomar alguns cuidados, com o objetivo de evitar a invasão da privacidade dos usuários do sistema. Um servidor de grande porte contém uma capacidade de armazenamento maior, o que tornaria proibitiva tal operação. O ideal é que seja definido um escopo, restringindo ao máximo a área de atuação da análise, evitando-se assim, violar a privacidade de inocentes (GUIMARÃES et al., 2001).

2.4 Implicações Legais

Conforme Guimarães et al., (2001) o perito deve seguir as normas contidas no Código de Processo Penal, destacando-se duas normas, a nível de exemplos.

> Art. 170. Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.

É sempre possível fazer cópias assinadas digitalmente das mídias que estão sendo investigadas para que possam ser feitas análises futuras, sendo necessário. O interessante é sempre atuar em cima de cópias, como será visto na sessão seguinte.

> Art. 171. Nos crimes cometidos com destruição ou rompimento de obstáculo a substração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.

Existe a necessidade de documentar quais as ferramentas de software utilizadas para fazer a análise, bem como a possível identificação de uma linha de tempo, que pode vir a ser conseguida através da análise do MAC time (linha de tempo).

Estes paralelos podem ser feitos visando garantir o valor judicial de uma prova eletrônica, enquanto não se tem uma padronização das metodologias de análise forense padronizadas.

2.5 Padronização na Aquisição de Evidências

Principais Entidades - As principais entidades que lidam com a investigação forense são: (1) International Organization on Computer Evidence (IOCE): principal entidade internacional centralizadora dos esforços de padronização; (2) Scientific Working Group on Digital Evidence (SWGDE): criado em 1998, ele é o representante norte americano nos esforços de padronização conduzidos pela IOCE; (3) High Technology Crime Investigation Association (HTCIA): organização sem fins lucrativos que visa discutir e promover a troca de informações que possam auxiliar no combate ao crime eletrônico; (4) International Association of Computer Investigatibe Specialists (IACIS): trata-se de uma associação sem fins lucrativos, composta por voluntários, com o intuito de atuar no treinamento em forense computacional; (5) Seção de Apuração de Crimes por Computador (SACC): atua no âmbito do Instituto Nacional de Criminalística/Polícia Federal, a fim de dar suporte técnico às investigações conduzidas em circunstâncias onde a presença de materiais de informática é constatada (OLIVEIRA, 2002)..

Padronização Internacional - Atualmente existem padrões definidos que são aplicados de forma experimental. Estes padrões foram desenvolvidos pelo SWGDE e apresentados na International Hi-Tech Crime and Forensics Conference (IHCFC), realizada em Londres, no período de 4 a 7 de outubro de 1999. Os padrões desenvolvidos pelo SWGDE seguem um único princípio, o de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiança e a exatidão das evidências. Este nível de qualidade pode ser obtido através da elaboração de Standard Operating Procedures (SOPs), que devem conter os procedimentos para todo tipo de análise conhecida, e prever a utilização de técnicas, equipamentos e materiais aceitáveis pela comunidade científica (SWGDE, 2000).

Padronização Brasileira - As instituições que encontram-se envolvidas em um esforço de padronização nacional são: Network Information Center (NIC) - Brazilian Security Office (NBSO) que atua coordenando as ações e provendo informações para os sites envolvidos em incidentes de segurança, foi criado em junho de 1997 (HOEPERS; STEDING-JESSEN, 2002);

Centro de Atendimento a Incidentes de Segurança (CAIS); que tem por missão o registro e acompanhamento de problemas de segurança no backbone e PoPs da RNP, incluindo auxílio à identificação de invasões e reparo de danos causados por invasores. Cabe, ainda, ao CAIS a disseminação de informações sobre ações preventivas relativas a segurança de redes e o Grupo de trabalho em segurança do comitê gestor da internet brasileira (CAIS, 2011).

2.6 Legislação

Ainda não existem leis específicas com relação aos crimes digitais, porém são aplicadas as leis existentes relacionadas a crimes que podem ser interpretadas para o meio digital. Os crimes digitais têm sido enquadrados na lei em itens como: estelionato, formação de quadrilha, quebra de sigilo, dano, escuta telemática, entre outros. A seguir, encontram-se relacionadas algumas leis utilizadas para punir os criminosos digitais.

Lei nº 9296/1996, em seu artigo 10º, determina que é crime uma pessoa interceptar ou apenas monitorar tráfego de comunicação de outra pessoa sem possuir uma autorização judicial. “Art.10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei” (L9296/96). Diversos fraudadores poderiam ser enquadrados nesse artigo, pois para conseguirem obter senhas e/ou outras informações confidenciais da vítima, ele precisará interceptar ou monitorar o tráfego de Internet para roubar as informações quando a vítima digitar ou enviar para outra pessoa. O acesso às informações pessoais da vítima, seja descobrindo sua senha para acessar seus e-mails, invadindo servidores para busca de informações pessoas de uma pessoa ou um grupo, ou apenas com a intenção de analisar o tráfego em uma rede privada, com o auxílio de ferramentas de monitoração de tráfego de rede, pode ser classificado como infração do artigo em questão, pois em um tráfego de uma rede provavelmente terão muitos dados privados ou até secretos, como senhas. (TREVENZOLI, 2006). A criação de cookies na máquina de um usuário que tem como função o monitoramento do hábito de navegação das pessoas pode ser classificada neste artigo, pois se trata de violação de privacidade (PL6827/06).

Lei nº 2848, em seu artigo 153, determina que "Divulgar alguém, sem justa causa, conteúdo de documento particular, ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano" (L2848/40). Existem certos vírus que tem

como característica enviar e-mails para as pessoas do catálogo de endereços da vítima, com trechos de e-mails enviados ou recebidos por outras pessoas ou colocar no corpo da mensagem fragmentos de textos que podem ser confidenciais. Neste caso o criminoso responsável pelo envio do e-mail poderia ser punido com base neste artigo, pois estaria divulgando informações confidenciais, sigilosas ou simplesmente particulares (TREVENZOLI, 2006).

Lei nº 2848, em seu artigo 155, determina que "Subtrair, para si ou para outrem, coisa alheia móvel" (L2848/40). Quando um fraudador obtém, de forma ilícita, os dados e a senha da vítima e realiza um desvio de dinheiro de contas bancárias, está cometendo um delito que pode ser classificado nesse artigo, pois se trata de um furto. Se houver destruição ou rompimento de obstáculo para o roubo da informação, ou se a vítima de alguma maneira facilitar o acesso às informações devido a confiança que tem no ladrão, ou quando o roubo é feito mediante tentativa de enganar a vítima são várias maneiras de conseguir o sucesso no furto e pode gerar uma ação judicial baseada neste artigo (TREVENZOLI, 2006).

Lei nº 2848, em seu no artigo 156, determina que "Subtrair o condômino, co-herdeiro ou sócio, para si ou para outrem, a quem legitimamente a detém, a coisa comum" (L2848/40). Quando o atacante obtém arquivos, dados pessoais confidenciais ou qualquer outra informação que seja pessoal e sigilosa, ele pode ser enquadrado nesse artigo, pois se caracteriza um roubo, visto que a vítima não deixou explícito que concordava com isso (TREVENZOLI, 2006).

Lei nº 2848, em seu artigo 163, determina que "Destruir, inutilizar ou deteriorar coisa alheia" (L2848/40). O fraudador que criar ou propagar um vírus destruidor, que formate o disco rígido ou destrua os arquivos pessoais da vítima, pode ser punido com base neste artigo. Não apenas vírus, mas outros códigos maliciosos como spywares, cavalos de tróia, worms, keyloggers, ou alterações em arquivos do sistema operacional podem destruir o computador da vítima (TREVENZOLI, 2006). Por exemplo, através de um cavalo de tróia enviado por um fraudador, outros atacantes podem se aproveitar desse código malicioso instalado para abrir as portas de comunicação da vítima podendo além de roubar informações, enviar comandos para destruir todos os dados contidos no computador (TREVENZOLI, 2006). Se um hacker realizar um ataque de negação de serviço, invadir um sistema de informática de uma empresa, ou um computador pessoal e realizar algum dano, que inviabilize o funcionamento do sistema

operacional ou de algum programa de computador específico, interromper os serviços do antivírus e outros softwares de segurança, ele pode ser classificado neste artigo, pois fatalmente vai gerar algum dano para o sistema de informática atacado (PL3016/00). Há alguns ataques a redes de empresas, realizadas a pedido de outra empresa concorrente, que tem a intenção de alterar dados verdadeiros para prejudicar de diversas maneiras a empresa atacada devido ao fato da empresa poder tomar decisões baseadas em dados errôneos. Esse ato pode ser classificado neste artigo (TREVENZOLI, 2006).

Lei nº 2848, em seu artigo 171, determina que "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento" (L2848/40). A obtenção de vantagens sendo através de roubo de senha, cartão de crédito, acarretando desvio de dinheiro pode ser enquadrado nesse artigo, pois esses crimes visam o benefício financeiro do criminoso. No estelionato o fraudador engana a vítima com o objetivo de conseguir vantagem patrimonial indevida acarretando em prejuízo, por isso muitos phishings são enviados trazendo um texto na tentativa de iludir a vítima para, que a mesma acesse o link recebido no scam. Com isso, se for um site de banco, essa pessoa digitará sua senha em um ambiente fraudulento, levando essa informação ao conhecimento do fraudador. Devido a ele ter se utilizado de mentiras para induzir a vítima a fornecer seus dados, seja num link de banco ou outro qualquer, que se trate de uma fraude, pode ser classificado neste artigo, pois se caracteriza um estelionato (TREVENZOLI, 2006).

Lei nº 2848, em seu artigo 307, determina que "Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem" (L2848/40). Quando um fraudador obtém a senha de alguma pessoa e a utiliza se fazendo passar pela pessoa, dona da senha, ele está realizando um crime, previsto nesse artigo, pois fingir ser uma pessoa é se atribuir de falsa identidade. O envio de e-mails, forjando a identidade de outra pessoa, também pode ser enquadrado nesta lei, pois se trata de utilização de falsa identidade, o que leva o remetente a abrir o e-mail, provavelmente carregando código malicioso, confiando-se na identidade do remetente. Outra situação de enquadramento neste artigo refere-se à informação de dados falsos ao realizar uma compra em alguma loja virtual. Como se trata de um cadastro de dados pessoais, sendo possivelmente criada uma cobrança no nome do cliente, a informação de dados falsos pode ser considerada crime (TREVENZOLI, 2006).

Lei nº 2848, em seu no artigo 288, determina que “Associarem-se mais de três pessoas, em quadrilha ou bando, para o fim de cometer crimes" (L2848/40). O crime de quadrilha ou bando configura-se quando mais de três pessoas, ou seja, no mínimo quatro pessoas, se organizam para a prática do crime. Se quatro ou mais pessoas se unem para a prática de um crime de informática, por exemplo, o desvio de dinheiro de várias contas em um banco, todos podem ser enquadrados com base neste artigo, pois se trata de uma união estável de quatro pessoas com o mesmo propósito, de cometer aquele crime juntos (TREVENZOLI, 2006).

Lei nº 2848, em seu artigo 313-A, determina que “Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano" (L2848/40). Podem ser classificados neste artigo, os funcionários autorizados que inserem ou facilitam a inserção de dados falsos, ou que exclui ou altera dados corretos em um sistema de banco de dados da Administração Pública (TREVENZOLI, 2006). Um exemplo disto é o caso do estagiário, estudante de direito, George Moreira Filho, que desviou três milhões de reais do INSS através de inserção de dados falsos realizando transações que beneficiavam seus familiares e amigos, com senhas de outros servidores, que ele descobriu de alguma forma (DACAUAZILIQUÁ, 2005).

Segundo Reinaldo Filho (2004), apesar de muitos crimes virtuais já serem cometidos similarmente na vida real, há vários crimes de informática novos que não possuem uma versão real, são realmente atuais, gerando a necessidade de alterações nas leis existentes para uma “atualização”, até mesmo dos termos, por exemplo, ampliando a definição do termo coisa para “dados”, “informação” e “senha”.

2.7 Identificação da Autoria

A identificação de autoria de um crime virtual é uma tarefa complexa e precisa de uma investigação minuciosa, pois qualquer informação pode ser uma pista importante. Devido a não existência de uma lei específica, os provedores de Internet no Brasil não são obrigados a manterem um registro detalhado de todos os acessos e conexões realizadas, o que pode produzir um prejuízo significativo nas investigações realizadas.

> Para acessar a Internet, qualquer pessoa precisa conectar-se a um provedor utilizando uma conta de acesso formada pelo nome de usuário e senha. No ato da conexão, o provedor atribui um endereço IP ao usuário, que o utilizará até encerrar a conexão. "Através do endereço IP, o provedor registra cada acesso do usuário, guarda seu nome de usuário, data e hora da conexão e desconexão. [...] Quando o acesso é feito através de ligação telefônica, os provedores também guardam, por meio de um sistema de identificação de chamadas, o número do telefone utilizado para estabelecer a conexão, o que garantiria a identificação em provedores gratuitos que utilizam uma conta padrão para o acesso à Internet (COSTA, 2004, p. 1).

Assim que uma fraude é detectada e as informações referentes ao provedor utilizadas para a conexão com a *Internet* (através do endereço *IP* de origem da fraude, ataque ou *e-mail* fraudulento enviado) são obtidas, a polícia recorre à Justiça em busca de uma ordem judicial solicitando os arquivos de registros junto ao provedor, a fim de conseguir identificar informações relativas à conta utilizada para conexão, que recebeu o *IP* naquele momento do envio do *e-mail*.

> O problema é que mesmo de posse de uma ação judicial, determinando que o provedor deva disponibilizar os arquivos de registros, os mesmos alegam não possuir mais essas informações referentes ao período solicitado, pois já foram substituídos por arquivos mais recentes, devido à falta de espaço em disco ou de mídias de armazenamento. Como não é obrigatório por lei, os provedores não são responsabilizados por essa falta de armazenamento de possíveis provas importantes (COSTA, 2004, p. 1).

Para que a investigação em busca da identidade do autor do crime seja cada vez mais eficaz e consiga desvendar grande parte dos crimes cometidos, é necessário, também, que haja uma interação entre as polícias de todos os países.

2.8 Medidas de Prevenção

Os criminosos virtuais dedicam seu tempo e focam seus ataques na tentativa de enganar os usuários, pois geralmente quando ocorre uma fraude é decorrente de falta de prevenção e conhecimento do usuário. Usuários com pouco conhecimento, ou até mesmo os mais experientes, geralmente não lêem todas as telas de tomadas de decisão quando acessam um site. Solicitações de instalações de plug-ins, active X56 (conjunto de tecnologias (*software*) criado para facilitar a integração entre diversas aplicações), e outras ferramentas, muitas vezes podem ser instalações de programas com código malicioso que o usuário nem se dá ao trabalho de ler e clica no botão padrão em evidência que geralmente é o "Sim".

.

O criminoso pode tentar atacar a entidade bancária, mas é bem mais fácil atacar a outra extremidade, o usuário. Além de realizar seus acessos confidenciais (bancos, compras, etc) de

uma máquina insegura, muitas vezes sem firewall[†] e com antivírus desatualizado, os criminosos ainda contam com a engenharia social a favor deles, pois ludibriar usuários com poucos conhecimentos em informática não é uma tarefa muito difícil, infelizmente.

Como o usuário é ainda o elo mais fraco e geralmente o atacado numa fraude eletrônica de *Internet Banking*, há soluções adicionais adotadas pelas instituições financeiras como exemplo: adoção de dispositivos como *OTP* (*One Time Password*) no qual o usuário recebe esse dispositivo que lhe informa uma nova senha a cada acesso ao *Internet Banking* (TREVENZOLI, 2006).

De acordo com Lau; Sanchez (2006) uma das opções adotada é a certificação digital, "composto por uma chave privada[‡]", que pode ser armazenada no sistema operacional ou dispositivo que permite apenas a inserção do dado cifrado resultando sua decriptação, não permitindo extração ou leitura da chave privada.

O objetivo das instituições financeiras não é de se isentar das responsabilidades e sim de tentar garantir a segurança nas transações bancárias, no entanto a adoção do uso do certificado digital pode ser perigosa para os usuários que não entendem o seu funcionamento. Mesmo que o uso do certificado digital dificulte bastante as fraudes ele não as isenta porque ele pode ser roubado.

Existem vários tipos de certificados, os quais se diferem pela maneira como foram gerados, onde são armazenados e pelo valor pago para emissão. O certificado com menor valor é o chamado A1, que fica armazenado no próprio computador, podendo ser roubado caso o computador esteja infectado com algum código malicioso, provavelmente um cavalo de tróia, que permita um acesso maior de controle ao computador.

De acordo com Siqueira (2006) há uma boa e uma má notícia para os correntistas usuários ou futuros usuários de meios eletrônicos para se comunicar com os bancos. A primeira é que, segundo especialistas e as instituições financeiras, as novas ferramentas de segurança são capazes, pela primeira vez, de reduzir sensivelmente os casos de fraude *on-line*, que até agora cresceram sem parar.

[†] É uma solução necessária para qualquer computador que se conecta a Internet. Tem como funcionalidade principal a proteção da rede ou da máquina (no caso de um firewall pessoal) contra ataques mal intencionados de pessoas através da Internet.

[‡] Chave privada é uma das chaves utilizadas no processo de criptografia assimétrica.

É possível verificar que há diversos métodos, ferramentas com tecnologia avançada que podem ser usadas isoladamente ou em conjunto para garantir maior eficiência na tentativa de inibir as fraudes, no entanto, de nada adianta fortalecer o meio digital com recursos muitas vezes de alto custo se a extremidade mais vulnerável – a do usuário, o ser humano, continuar com o mesmo nível baixo de conhecimento técnico.

Para tentar atingir o objetivo de melhorar a segurança nas transações bancárias, as instituições financeiras devem investir ainda muito mais no aumento de conhecimento dos clientes para que os mesmos sejam mais desconfiados com o que lêem na *Internet*, como são atualmente na vida real (TREVENZOLI, 2006).

Segundo Lau (2006) é preciso que os órgãos públicos de repressão atuem constantemente na investigação e punição, com apoio da imprensa para divulgar as operações.

3 METODOLOGIA

Este estudo foi desenvolvido seguindo a metodologia qualitativa, tipo descritivo, por meio de uma revisão bibliográfica. Lüdke; André (2001) afirmam que, o estudo qualitativo é rico em tópicos descritivos possibilitando um estudo com perguntas abertas e flexíveis, observando toda a realidade contextualizada.

Realizou-se, neste estudo, um levantamento bibliográfico em sites técnicos especializados e atualizados de periódicos, de anais de congressos, de fóruns ambientais, de informativos técnicos, de livros, de diretrizes, de lei, de projetos de leis e publicações em geral, dos principais conceitos relacionados com o tema. Buscou-se as informações por meio dos seguintes termos de pesquisa em combinações diversas: análise forense, forense computacional, NBSO, CAIS, Perícia Forense Computacional, Forense Digital, Investigação Eletrônica.

4 ANALISE E INTERPRETAÇÃO DOS

Neste milênio, pessoas de todas as classes e lugares passaram a ficar a cada vez mais próximas das tecnologias de comunicação e armazenamento e cada vez mais, acessam a

grande rede através de computadores instalados em suas casas, no trabalho e em lugares públicos.

A literatura mostra que o desafio hoje para as empresas, é a invasão de crackers ansiosos por roubar informações confidenciais valiosas, observando que as ameaças além de crescerem, estão mais poderosas. Para os usuários, que geralmente não são cuidadosos com os seus dados, as informações podem ser mal utilizadas, o que o torna uma grande preocupação.

Os criminosos virtuais dedicam seu tempo e focam seus ataques na tentativa de enganar os usuários, pois geralmente quando ocorre uma fraude é decorrente de falta de prevenção e conhecimento do usuário. Na realidade, as atividades criminosas em computadores são crescentes e avançadas.

Talvez tenha chegado a hora da Tecnologia da Informação a repensar a segurança da rede, no sentido de como obter e utilizar evidências digitais no amparo efetivo à justiça, pois muitas são as dificuldades da perícia forense computacional para ser mais eficiente e precisa, podendo-se considerar a falta de legislação específica, procedimentos não padronizados, negligência dos usuários, poucos especialistas como dificuldades principais dentre outras existentes.

4 CONSIDERAÇÕES FINAIS E SUGESTÕES

A questão levantada neste estudo que tem como base a segurança na Internet possibilitou a elaboração do seguinte problema: Existe necessidade da disciplina Forense computacional? Os estudos sobre este tema favorecem a investigação, a prevenção e proteção das informações?

Este estudo teve como objetivo geral analisar os principais conceitos e ferramentas utilizadas pela perícia forense computacional, para auxiliar na coleta, manutenção e análise de evidências digitais para promover a reconstituição dos eventos encontrados e como objetivos específicos apresentar conceitos e noções de forense computacional e descrever ferramentas aplicadas na forense computacional.

Neste estudo pode-se verificar que:

Com a expansão da Internet e, conseqüentemente, o aumento de crimes eletrônicos surgem questões sem respostas, sendo que a quantidade de profissionais desta área não é suficiente para apurar os atos ilícitos cometidos diariamente.

O parco conhecimento específico sobre a forense computacional é um dos fatores visíveis para a realização deste estudo. Por isso, a disseminação dos conceitos é importante no campo de segurança da informação, de forma a complementar as regras e definições dentro dessa área.

A falta de padronização e a ausência de normas podem possibilitar erros para evidências despercebidas; e por vezes pode existir dúvidas do que se pode usar legalmente.

A necessidade da forense computacional se deve ao fato de que não se existe um computador ou dispositivo totalmente seguro, fazendo, obviamente, com que os intrusos deixem rastros. Assim, os estudos e práticas sobre a área só tendem a favorecer tanto o perito como o dono do sistema invadido, possibilitando-os a prevenção e proteção das informações.

Sugere-se que as empresas invistam em treinamentos de funcionários para a aquisição, a examinação e a utilização adequada da evidência eletrônica, possibilitando-os a prevenção e aplicações protetoras das informações. Que invistam, também, em estudos e na divulgação dos achados sobre o tema, de forma que possam contribuir com a prevenção e proteção dos usuários físicos. E por fim sugere-se a Tecnologia da Informação a repensar a segurança da rede, no sentido de como obter e utilizar evidências digitais no amparo efetivo à justiça.

REFERÊNCIAS

ANDRADE, M. M. **Introdução à metodologia do trabalho científico:** elaboração de trabalhos na graduação. 6. ed. São Paulo: Atlas, 2003.

BESSA, L. **Websense revela suas previsões sobre a segurança da internet para 2007**. IMS Marketing. Websense, Inc. Disponível em: http://www.websense.com/global/pt/PressRoom/PressReleases/PressReleaseDetail/index.php?Release=0612191332, 2006.

CAIS - **Centro de Atendimento a Incidentes de Segurança.** 2011. Disponível em <http://www.cais.rnp.br> Acesso em: 04 jun. 2011.

COSTA, M.A.S.L. **Mundo virtual sem lei**, 04/02/2004. Instituto de Criminalística Afrânio Peixoto (ICAP). Departamento de Polícia Técnica da Bahia. Disponível em: <http://www.dpt.ba.gov.br/dpt/web/ICAPInterna.jsp?CId=1282&ModId=70> Acesso em: 02 jun. 2011.

DACAUAZILIQUÁ, José. **Estagiário desvia R$ 3 milhões do INSS**, Associação Nacional das Entidades Associativas dos Servidores da Polícia Federal, 30/11/2005. Disponível em: <http://www.ansef.org.br/verNoticia.php?cod=299> Acesso em: 03 jun. 2011.

FREITAS, A.R. de. **Perícia Forense Aplicada à Informática.** Pós - Graduação "Lato Sensu"em Internet Security, Instituto Brasileiro de Propriedade Intelectual, IBPI, 2003. Disponível em: <www.linuxsecurity.com.br/info/general/andrey-freitas.pdf.> Acesso em: 04 jun. 2011.

GUIMARÃES, C. C. et al. **Forense computacional:** aspectos legais e padronização. Disponível em: <http://bastion.las.ic.unicamp.br/paulo/papers/2001-WSeg-flavio.oliveira-marcelo.reis-forense.pdf> Acesso em: 04 jun. 2011.

L2848/40. **LEI Nº 2.848, DE 07 DE DEZEMBRO DE 1940.** Associação do Ministério Público do Estado do Rio de Janeiro. Disponível em: <http://www.amperj.org.br/store/legislacao/codigos/cp_DL2848.pdf> Acesso em: 01 jun. 2011.

L9296/96. **LEI Nº 9.296, DE 24 DE JULHO DE 1996.** Presidência da República. Disponível em: < https://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm> Acesso em: 05 jun. 2011.

LAU, M. **Análise das fraudes aplicadas sobre o ambiente Internet**
LEI Nº 12.228, DE 11 DE JANEIRO DE 2006. Ministério Público – Estado do Rio Grande do Sul. Disponível em: <http://www.mp.rs.gov.br/consumidor/legislacao/id2316.htm> Acesso em: 02 jun. 2011.

LUDKE, M.; ANDRÉ, M. E. D. A. **Pesquisa em educação:** abordagem qualitativas. São Paulo: EPU, 1986.

MINAYO, M. C. S. **O desafio do conhecimento:** pesquisa qualitativa em saúde. 8. ed. São Paulo: Hucitec, 2004.

NOBLETT, M. G.; POLLITT, M. M.; PRESLEY, L.A.; *Recovering and Examining Computer Forensic Evidence*; **Forense Science Communications;** Federal Bureau of Investigation; v. 2, n. 4, out., 2000. Disponível em: http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/oct2000/computer.htm#Top of article. Acesso em: 02 jun. 2011.

OLIVEIRA, F. de S. **Resposta a incidentes e análise forense para redes baseadas em Windows 2000**. Dissertação (Mestrado em Ciência da Computação) - Universidade Estadual de Campinas, Instituto de Computação, 2002. Disponível em: <http://bastion.las.ic.unicamp.br/paulo/teses/20021121-MSc-Flavio.de.Souza.Oliveira-

resposta.a.incidentes.e.analise.forense.para.redes.baseadas.em.Windows.2000.pdf.> Acesso em: 04 jun. 2011.

PEREIRA, E. et al. **Forense Computacional**: fundamentos, tecnologias e desafios atuais. In: Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 3, 2007. Universidade do Vale do Rio dos Sinos – Unisinos, 2007.

REINALDO FILHO, D. **O projeto de lei sobre crimes tecnológicos (PL nº 84/99). Notas ao parecer do Senador Marcello Crivella.** Jus Navigandi, Teresina, ano 9, n. 375, 17 jul. 2004. Disponível em: <http://jus.uol.com.br/revista/texto/5447>. Acesso em: 9 jun. 2011.

SWGDE - Scientific Working Group on Digital Evidence; IOCE, International Organization on Digital Evidence; **Digital Evidence:** Standards and Priciples; Forense Science Communications, v. 2, n.2, abr., 2000.