Perícia Forense Computacional

Luciano Cordova Tolentino, Wanessa da Silva e Paulo Augusto M. S. Mello

***Resumo*—As proporções alcançadas pelo meio tecnológico são enormes, onde praticamente tudo em um mundo informatizado funciona a base de programas de desenvolvimento de software, em que celulares podem acessar a internet de qualquer lugar e até geladeiras tem um programa lógico para mostrar as horas. Com a tecnologia tão imponente no mundo, também se encontram os criminosos que as usam para cometer delitos a toda e qualquer pessoa nesse meio. Peritos forenses computacionais executam suas finalidades para desvendar quem são os criminosos através de investigações específicas não deixando a impunidade livre no meio virtual. Esse trabalho explana especificamente a importância do perito e as fases percorridas por eles para chegar a uma solução, bem como desvendar crimes que parecem impossíveis quando se fala em procurar *bits* como prova. Esse artigo não tem o objetivo de esclarecer totalmente, mas de dar uma noção de como esses profissionais trabalham gerando assim a curiosidade das pessoas instigando-as a novas pesquisas mais abrangentes nessa área.**

***Palavras-chave*— Perito Forense, Perícia Forense Computacional, Crimes Cibernéticos, Evidências Digitais.**

I. Introdução

COM o avanço tecnológico de ferramentas para intrusões de sistemas, os crimes virtuais obtiveram força e, consequentemente, êxito nos ataques efetuados. Para prevenir e até mesmos extinguir os ataques virtuais, peritos especializados utilizam técnicas forenses como forma de combate.

A perícia forense aplicada à computação é ligada a investigação de crimes cibernéticos colhendo dados para identificação, preservação, análise e documentação com a finalidade de obtenção de evidências digitais.

Alguns procedimentos devem ser seguidos pelo perito para assegurar que a evidência não seja comprometida, substituída ou perdida (Freitas, 2007).

Os profissionais na área têm regras a seguir, providências definidas a tomar, para obter credibilidade no que faz, artigos específicos de como um capacitado deve proceder em uma investigação para que seu trabalho não tenha sido em vão e desconsiderado em uma audiência judicial, onde um parecer técnico será necessário. Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados (Queiroz & Vargas, 2010).

P.A.M.S. Mello é professor da Escola de Tecnologia da Faculdade Projeção. Contato: paulo.meloespam@projecao.br.

Por conter pouca informação registrada em lei e grande parte das pessoas, inclusive as que estão ligadas à tecnologia não entender o significado do termo perícia forense computacional, resolvemos abordar sobre o que é e quais procedimentos devem ser realizados pelos peritos ao se procurar uma informação confidencial. O projeto foi executado pensando também na sociedade que ganhará um artigo científico abordando sobre um tema não tratado cotidianamente. O objetivo desse trabalho é mostrar de forma breve a importância do perito forense computacional, como o trabalho dos peritos é importante na busca e nas soluções de crimes, focado principalmente nas soluções de fraudes ligadas à informática e como efetua as perícias (procedimentos, técnicas e programas utilizados).

II. Metodologia

O método utilizado nessa pesquisa foi a revisão bibliográfica, leitura e interpretação de alguns autores, dentre eles se encaixam (Freitas, 2007), (Queiroz & Vargas, 2010), (Farmer & Venema, 2007), (Scudere, 2007) e alguns artigos já publicados, em meio a eles estão: Perícia Forense Aplicada à Informática de Andrey Rodrigues de Freitas em 2007; Forense Computacional: Aspectos Legais e Padronização em 2008; Perícia Contábil: aspectos técnicos, legais e éticos, Daniel Mello em 2009.

III. O Que é Perícia?

É a prática que um profissional qualificado exerce, neste caso denominado de perito. Vistoria ou exame de caráter técnico e especializado. Conhecimento, ciência (Dicionário Aurélio, 2009).

O perito averigua e investiga os fatos de uma ocorrência e propõe um laudo técnico para entendimento geral de um episódio, comprovado através de provas. Existem variados tipos de peritos: criminal, ambiental, de medicina, de tecnologia, dentre outros. Cada um atuando em sua área e trazendo provas concretas de um evento ocorrido, contento detalhes e um parecer de um especialista na área. No geral, eles juntam peças importantes para descobrir a origem de um crime ou para desvendar algo que não está concreto.

A averiguação é acionada quando se faz necessário a comprovação de um crime, através de análises de documentos, testemunhas, objetos e exames. Um laudo ou um relatório técnico imparcial é gerado para que fiquem claras as comprovações dos fatos fundamentados, de forma a nortear os julgadores do acontecido.

Um perito é convocado quando a resolução de um delito não fica clara e, em casos de ações judiciais, é escolhido por um juiz para o caso especifico. A perícia age quando é necessário um laudo de um especialista no assunto, busca de fatos e provas para esclarecer o que aconteceu no local.

IV. O TERMO FORENSE

Segundo o professor Candido Fonseca da Silva da Unisinos – São Leopoldo – RS "*Forense é a ciência dividida em diversas disciplinas, que atua em conjunto com o investigador na busca pela verdade*". A Ciência Forense é desenvolvida por profissionais altamente qualificados e especializados, em que as pistas deixadas no local do crime só são atestadas como verídicas após testes em laboratórios. Criminosos a cada dia cometem seus delitos de forma a não deixar vestígios e, em casos como esse, a perícia forense opera nas descobertas de pistas que não podem ser vistas a olho nu, na reconstituição de fatos em laboratórios seguindo as normas e padrões pré-estabelecidos para que as provas encontradas tenham validade e possam ser consideradas em julgamento de um processo.

Forense computacional visa os mesmos eventos relatados acima só que na área tecnológica, buscando pistas virtuais que possam descrever o autor das ações não permitidas.

A Forense Computacional foi criada com o objetivo de suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. Ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional (Guimarães et al., 2008).

V. PROCEDIMENTOS E MÉTODOS APLICADOS A PERÍCIA FORENSE COMPUTACIONAL

Segundo Andrei Rodrigues de Freitas (2007), a perícia forense possui quatro procedimentos básicos: todas as evidências devem ser (a) identificadas, (b) preservadas, (c) analisadas e (d) apresentadas. No caso de crimes cometidos através de um computador, as evidências normalmente são dados lógicos e virtuais, cabendo ao perito identificar de forma correta e aplicável ao meio que se encontra como preservar e armazenar essas provas. Não necessariamente devem-se utilizar todas as etapas descritas acima. Pode-se utilizar somente uma etapa, a maioria ou todas elas.

Existem inúmeros crimes virtuais e, consequentemente, há diversas evidências que o perito necessita avaliar se é ou não necessário para o laudo técnico pericial.

Na identificação, o perito deve-se atentar para o tipo de crime praticado. Por exemplo, o perito buscará por evidências de *logs*, conexões, alteração de arquivos confidenciais, caso o crime seja de acesso não autorizado. Caso o crime seja de pornografia com menores, o perito deve identificar imagens e vídeos no HD do usuário, verificar o histórico e arquivos temporários do navegador. Portanto, ao identificar uma evidência digital, a parte física - *hardware* - do computador ou de equipamento digital é de muita importância para descobrir provas e pistas.

Existe a análise ao vivo que consiste na perícia do equipamento a ser averiguado ainda em funcionamento. Nesses casos, o perito deve atentar para os processos que estavam em execução no momento e as portas abertas pela rede. Na etapa de preservação, a veracidade da evidência é o principal foco dos peritos. Para se garantir que não foram alterados, substituídos, perdidos ou corrompidos os dados, utiliza-se a Cadeia de Custódia.

Assim, a Cadeia de Custódia viabiliza o controle sobre o trâmite da amostra com a identificação nominal das pessoas envolvidas em todas as fases do processo, caracterizando as suas responsabilidades, as quais são reconhecidas institucionalmente, uma vez que, como já foi citado, as mesmas foram treinadas para estas atividades. Portanto, o fato de assegurar a memória de todas as fases do processo, constitui um protocolo legal que permite garantir a idoneidade do resultado e rebater as possíveis contestações. (Lopes et al, 2008).

FORMULÁRIO DE CADEIA DE CUSTÓDIA

NÚMERO DO CASO	20090226		
DETALHES DA MÍDIA OU EQUIPAMENTO			
ITEM	DESCRIÇÃO		
1	HD DO NOTEBOOK COM 2 GB DE CAPACIDADE		
FABRICANTE	MODELO	NÚMERO DE SÉRIE	
SAMSUNG	SGM2GB	ABC123456	
SOBRE A IMAGEM DOS DADOS			
DATA	HORA	CRIADA POR	FERRAMENTA USADA
26/2/2009	10:53	SÍLVIO DO MONTE	EnCASE VERSION 3
TIPO DE CÓPIA	HASH		
DISCO COMPLETO	4e3d2d5e5427953d7eda6ddc6627bf6b		

CADEIA DE CUSTÓDIA						
CÓDIGO	ORIGEM	DATA	HORA	DESTINO	DATA	HORA
1	LOCAL DE APREENSÃO	26/2/2009	17:00	PERÍCIA	26/2/2009	17:30

Fig. 1. Exemplo de formulário de cadeia de custódia. http://forensics.luizrabelo.com.br/2011/08/cadeia-de-custodia.html.

Conforme o site http://dsconcursos.com.br/index.php?option=com_content&view=article&id=365:resumo-computacao-forense&catid=86:ti-seguranca-da-informacao&Itemid=129, concomitantemente, necessita-se de técnicas alternativas para futuras investigações em casos de equipamentos estarem sendo analisados "ao vivo", por exemplo. O perito deve realizar imagem dos dados voláteis, para preservar o estado inicial do equipamento inalterado e posteriormente realizar uma análise mais minuciosa, preservando as provas originais.

O cuidado com a evidência tem que ser extremamente alto durante o seu transporte. Quedas, alta temperatura,

líquidos e poeira causam danos à evidência acarretando a não veracidade da mesma. A prova após ter sido transportada deverá estar em local seguro e monitorado para garantir a inviolabilidade.

Freitas (2007) cita que a análise é uma das etapas mais importantes da perícia forense. Para facilitar a etapa de análise utilizam-se perguntas chaves que objetivam tal ato, como:

- Qual a versão do Sistema Operacional utilizado?
- Quem *logou* ou tentou *logar* no computador recentemente?
- Quais arquivos foram usados pelo suspeito?
- Qual porta estava aberta?
- Quais arquivos foram excluídos?

Toda evidência encontrada necessita ser documentada para validação e verificação. Por vezes, utiliza-se separação por prioridade das evidências (irrelevante, relevante, entre outros) que posteriormente serão usados como provas no tribunal competente.

A apresentação da análise é feita através do laudo técnico pericial em que devem constar os fatos, as evidências, os procedimentos, as análises e, obviamente, o resultado.

O laudo terá que ser claro, conciso e objetivo de forma que apresente as idéias e os culpados, quando houver, para dar uma linha de julgamento ao crime e um entendimento melhor das partes envolvidas deixando bem evidente o ocorrido.

VI. ANÁLISES FÍSICAS

São análises de artefatos físicos normalmente de mídias danificadas ou impossibilitadas de leitura, de teor desconhecido, em que é extraída a imagem e salva para análise posterior. Os testes que serão feitos ou leitura de dados importantes, como *logins* de usuários no HD, são feitos em cima dessa imagem ou de dados coletados pelo perito dentro da mídia e armazenados em outro local.

Análises lógicas

Na pesquisa lógica são analisados os arquivos das partições que consisti em usar um sistema operacional capaz de abranger o sistema de arquivos, com isso não são usados sistemas de uso comum como Windows e suas versões. Após a busca no arquivo, monta-se uma imagem restaurada no modo somente de leitura para não sofrer alterações.

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 (Freitas, 2007).

VII. ANÁLISES DOS SISTEMAS DE ARQUIVOS

Arquivos excluídos de sistemas podem ser persistentes e se manterem ocultos em algumas partes do HD por vários meses, mesmo que não se cometa movimentações ou acessos. A investigação de arquivos se baseia em conhecimento, em procurar pistas onde todos crêem que não se encontram mais no local, seguir o que foi ensinado e também seus próprios métodos de busca, não fugindo à regra, tendo em vista que se os conceitos de averiguação forem baseados somente em normas individuais, as análises terão sido em vão podendo não se aplicar dentro do julgamento do caso.

De acordo com Famer & Venema (2007), avaliações em cima de um sistema deverão ser feitas com dados mais legítimos possíveis e, seguindo esse preceito, é feita uma cópia do sistema para análise em que não se perca nada durante a investigação. A reprodução funciona como uma fotografia do local do crime antes de começarem a trabalhar em cima das provas. Cada ação provoca uma reação dentro do sistema, digamos que ao acessar um arquivo qualquer, com este simples ato, pode-se estar apagando dados que poderiam ser importantes na averiguação.

A análise forense tradicional se concentra nos dados dos sistemas que não estão em execução. A doutrina diz para desligar o sistema e copiar os dados que sobreviveram à transição: *logs* de programas, horários de acesso, o conteúdo dos arquivos e assim por diante. A análise é então feita em uma cópia dos dados, o que minimiza o perigo para o original. Essa abordagem facilita uma captura fácil dos dados e uma cadeia razoavelmente irrefutável da lógica ao demonstrar os resultados (Farmer, Venema, 2007).

Não cabem no ambiente cibernético os procedimentos certos de como fazer a coleta de informações, cada um faz como achar melhor, o que não seria o mais indicado na presença de um tribunal onde uma padronização seria o recomendado, mas uma singularidade na investigação individual pode trazer provas que outros peritos não puderam encontrar.

VIII. LAUDO PERICIAL

Os passos do perito antes, durante e posterior à investigação devem constar no laudo pericial, um documento que sugestiona de forma a aprovar ou reprovar as posições tomadas pelo perito durante o processo de investigação. No laudo constam as conclusões tomadas após minuciosas investigações através das comprovações em laboratório, trazendo um parecer verdadeiro detalhando tudo o que foi recolhido e investigado, a forma como fora feito a investigação e de como foi provada a veracidade dos artefatos recolhidos terminando com as conclusões tomadas pelo perito.

O Laudo pericial será elaborado no prazo máximo de 10 dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos (Queiroz & Vargas, 2010). O laudo pericial tem quer ser de entendimento de todos, inclusive do juiz que irá julgar o caso, levando em conta que o mesmo só entende do código de lei vigente e não de termos técnicos.

Queiroz & Vargas (2010) dizem que o laudo do perito

forense computacional é mais complexo que os demais por serem usados jargões que normalmente é entendido somente no âmbito tecnológico e palavras que não constam no dicionário da língua portuguesa. Se o laudo não for entendido pelos julgadores, pode ser requerido que seja novamente escrito e até mesmo ser pedido a troca do perito. Isso não implica na inutilização de linguajar técnico, apenas deve ser de entendimento de todos, sem interceptar a compreensão do laudo em sua totalidade.

IX. COLETA DE ARQUIVOS EM CELULARES

Celulares são inovadores e carregados de tecnologia, com possibilidades imensas de guardar dados pessoais dentro desses dispositivos. Já existem no mercado *smartfones* que variam de aplicativos de agenda, a acesso de *e-mails* através da *web*, os ataques contra esse tipo de aparelho pode causar amplos prejuízos ao usuário que armazena uma grande quantidade de informações particulares, esses ataques podem ser sofridos não apenas pelo dono do aparelho, mas também pelos demais contatos que o proprietário mantém salvo.

Temos hoje no mercado o Encase Portable, o Solo4 e agora é a vez do Field Version 2, dispositivo que atende os mais altos padrões do mercado mundial (MIL-801). Com menos de 4 kg, o Field Version 2 é projetado para os investigadores da cena do crime, unidades móveis de inteligência militar, policial e organizações internacionais, como a ONU. http://imasters.com.br/artigo/14325/gerencia-de-ti/dispositivo-movel-para-coleta-em-celulares.

A ferramenta não tem esta limitação de memória. Como as memórias de telefone são cada vez maiores (até agora 16-32Gb), esta limitação torna-se mais importante. Apresenta a possibilidade de verificar todos os dados diretamente como eles são salvos em um PC / portátil. http://imasters.com.br/artigo/12682/gerencia-de-ti/forense-digital-em-celulares

Em seu blog *imasters* Vargas ainda diz que com a ferramenta XRY / XACT é possível transformar os arquivos extraídos em variados documentos como, .doc .xls dentre outros, o que proporciona a gravação de dados em CD visando o armazenamento de informações para averiguações posteriores. Clona-se também o *chip* sem conectá-lo a nenhuma rede, portanto não receberá ligações.

A grande pressão para agilidade nos processos de diversas tipificações fez com que a justiça providenciasse ações concomitantes com peritos forenses computacionais para solucionar casos que demandem conhecimento técnico.

Encontrar empresas que fornecem esse tipo de serviço não é tão comum quando comparados com empresas de desenvolvimento de *software*. Segundo o site http://gilbertomelo.com.br/jurisprudencias-e-noticias/90/832-pericia-forense-ganha-espaco-nas-empresas, a ISSA - *Information System Security Association, sediada em Oak Creek, Wisconsin* (EUA) atua no Brasil com uma equipe de oito profissionais e atende uma média de 100 contratos anuais sobre forense computacional. A demanda empresarial é crescente e os preços dos contratos estão hoje numa faixa de 10 mil reais.

No Brasil, temos a Polícia Federal que auxilia a justiça quebrando senhas, recolhendo dados de HD's, análise e correlacionamento de dados com o objetivo de reconstruir ações e cenários, estabelecer causa e efeito, autoria, local e testemunhas, que depois transformarão em um laudo e ação judicial.

A empresa Clavis – Segurança da informação oferece de um modo geral implantação de sistemas seguros em redes de computadores, bem como análise forense, fornecem cursos de capacitação para sua equipe e para interessados, além de ministrar *wokshops* no país. Por ser uma empresa nova só possui uma loja situada no Rio de Janeiro.

X. DIFICULDADES NA COLETA DE DADOS

A *internet* é ilimitada e sem fronteiras. Uma pessoa pode cometer um crime do outro lado do mundo e afetar alguém aqui no Brasil, com isso dificulta muito o trabalho da perícia forense computacional, que diferente dos peritos de crimes habituais, que podem cercar a área e coletar dados finitos, o perito forense não tem limites, dependem não só dos dados, mas também da colaboração internacional em determinados casos.

Para se encontrar um criminoso através da internet pode ser uma tarefa bem árdua, contando que entre um criminoso e uma vítima pode conter mais de vinte e cinco endereços IPs onde muitos podem ser inválidos ou terem sido alterados, manipulados, para que quando houver as buscas se percam dentre esse emaranhado de endereços que existe na rede.

Vários diagramas podem ser construídos para demonstrar o trajeto de reconstrução de um caso de fraude tecnológica, cruzando países. Chamamos de *hopp*s cada conexão entre endereços IP (Scudere, 2007)

De acordo com Scudere (2007), as operadoras que fornecem ou controlam esses endereços IPs guardam os dados por curto prazo, consequentemente até que se consiga uma autorização do juiz para a coleta dessas informações, tudo pode ter sido em vão e a investigação não ter como prosseguir. Não se conta com padrões internacionais para esse tipo de evidência, o que dificulta muito em dizer o que é considerado prova de um crime cibernético e o que não é, onde provas recolhidas quando levadas a um julgamento pode ter valor irrelevante perante aqueles que irão julgar o caso.

Outro empecilho é a legislação que se diferencia para cada nação, o que é considerado crime em outros países pode não gerar penalidade alguma aqui no Brasil e vice e versa, portanto o julgamento de um criminoso de outro país

vai depender principalmente da colaboração mútua entre os países.

XI. LEGISLAÇÃO APLICADA À PERÍCIA FORENSE COMPUTACIONAL

Para ser um especialista em perícia forense é necessário estar ciente sobre a legislação brasileira vigente, em que vários casos é a lei que vai nortear o perito de como deve proceder, onde só a visão técnica não é o bastante para resolução do acontecimento. Segundo Guimarães (2008), as leis processuais brasileiras mostram o caminho que o perito deve percorrer e as condições estabelecidas para a formação de um profissional em forense, embora existam ainda muitas brechas na lei, já há artigos específicos para algumas situações.

"Art 421. Parágrafo 1º Os peritos serão escolhidos entre profissionais de nível universitário, devidamente inscritos no órgão de classe competente, respeitando o disposto no Capítulo VI Seção VII, deste código (Incluído pela Lei 7.270 de 10.12.1984)." (Queiroz & Vargas, 2010).

O profissional dessa área para ter excelência no que faz é necessário que conheça profundamente aquilo ao qual desenvolve, porque na forma de investigador, pode-se estar inserido nas mais diversas áreas da justiça, tendo que conhecer as leis a fundo para saber como proceder junto a uma determinada convocação do juiz, que variam desde áreas trabalhistas até processos penais. Sabendo sempre que estará ao lado de advogados e que sua opinião será relevada em um procedimento, como também seu laudo pode ser essencial na comprovação de um delito podendo ajudar nas considerações durante o julgamento.

Legislações em países estrangeiros X Legislação brasileira, ligadas a crimes virtuais

Invadir informações em um banco de dados não generaliza crime em potencial no Brasil, difundir essa informação sim, mas não há histórico de punições a este respeito dentro da legislação brasileira, constando como crime apenas aquela pessoa que detém os dados e os propagam, mas como os hackers não são os proprietários das informações nada acontecerá aos mesmos, pois não há lei que se aplica em nossa nacionalidade. Segundo o portal do G1 no site http://g1.globo.com/Noticias/Tecnologia.html "Não há no Brasil a tipificação de crime resguardando o banco de dados, proibindo adquirir, acessar, modificar, distribuir, vender ou disponibilizar banco de dados de terceiro, sem a devida autorização".

Nos Estados Unidos quem invade uma base de dados a fim de prejudicar de alguma forma os proprietários ou até mesmo só por conseguir o acesso, sofrem penas rigorosas que variam desde pagamentos de indenizações até retenção por vários anos.

"*O ex-universitário de Miami Albert Gonzalez, 28, confessou que ajudou a liderar um grupo global que roubou mais de 40 milhões de números de cartão de crédito invadindo sistemas de varejistas, incluindo TJX, BJ's Wholesale Club e Barnes & Noble*" (http://www1.folha.uol.com.br/folha/informatica/ult124u712092.shtml).

Uma notícia do dia 12/10/2011 que foi divulgada no site www.correioweb.com.br pode ser citada como exemplo de punições aplicadas nos Estados Unidos. *Recentemente Christopher Chaney, um hacker que conseguiu invadir e-mails de celebridades e difamar suas imagens foi preso e pode cumprir pena de até 121 anos de prisão, responderá também por 26 acusações dentre elas a de falsa identidade*.

XII. CONCLUSÃO

O acesso à informação digital está cada vez mais facilitado através da utilização da internet. Pessoas mal intencionadas utilizam esse recurso para ganhar dinheiro e até mesmo para cometer crimes na rede. Consequentemente, da mesma forma que existem policiais para deterem e investigarem crimes e furtos físicos, também existe peritos forenses que atuam na área contra crimes e investigações computacionais.

Este artigo se limitou a procurar fontes de pesquisas como embasamento para relacionar as atividades praticadas pelos profissionais forenses e sua importância no mundo informatizado como o atual, esclarecer dúvidas sobre a legislação vigente aqui no nosso país como comparativos outros países, crimes idênticos podem ser tratados de formas bem diferentes. O Brasil se encontra obsoleto em relação à legislação, por estar inserido no meio tecnológico, necessita de leis mais rigorosas contra criminosos desse meio.

Peritos têm métodos para encontrar informações contidas em *softwares*, no Brasil falta além de empresas qualificadas nessa área, ferramentas especializadas para a pesquisa detalhada e coleta de provas. A tecnologia evolui a cada ano, os criminosos têm acompanhado esse progresso, mas em contrapartida os investigadores não, por falta de investimento e desinteresse do país. As empresas que zelam pelos seus dados têm de recorrer a serviços particulares, ficar esperando por atitudes do governo nada ou pouquíssimo será feito.

Trabalhos futuros podem abordar temas mais complexos como ferramentas inovadoras para buscar dados, o avanço tecnológico que vem para ajudar, mas que pode prejudicar com o manuseio por pessoas más intencionadas, ações e leis mais severas que os governos devem investir para barrar as ações de criminosos, monitorar as redes para evitar a invasão ou para descobrir em menos tempo quem invadiu e por fim, mas não menos importante dar mais ênfase a crimes virtuais, pois são tão prejudiciais quanto um crime físico.

REFERÊNCIAS

FARMER, Dan; VENEMA, Wietse. Perícia Forense Computacional: Como Investigar e Esclarecer Ocorrências no Mundo Cibernético. Curitiba – SP: Ed. Pearson Prentice Hall, 2008.

FERREIRA, Aurélio Buarque de Holanda. Aurélio: O Dicionário da Língua Portuguesa. 8º Edição. São Paulo - SP: Ed. Positivo, 2009.

FREITAS, Andrey Rodrigues. Pericia Forense Aplicada à Informática. São Paulo – SP. Instituto Brasileiro de Propriedade Intelectual – IBPI, 2007.

FREITAS, Andrey Rodrigues. Pericia Forense Aplicada à Informática: Ambiente Microsoft. Rio de Janeiro - RJ: Ed. Brasport, 2007.

GUIMARÃES Célio Cardoso; OLIVEIRA, Flávio de Souza; REIS, Marcelo Abdalla; GEUS Paulo Lício de, Forense Computacional: Aspectos Legais e Padronização. Campinas – SP. Instituto de Computação – UNICAMP, 2008.

LOPES, M; GABRIEL, M.M. ; BARETA, G. M. S., Cadeia de Custódia: uma abordagem preliminar. Paraná – PR, UFPR, 2008.

QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e Pericia Forense Computacional: Certificações, Leis Processuais, Estudos de Caso. Rio de Janeiro – RJ: Ed Brasport, 2010.
SCUDERE, Leonardo. Risco Digital: como a tecnologia pode agregar valor, criar novas oportunidades e reduzir fraudes. Rio de Janeiro - RJ: Ed. Campos, 2007.

<http://www.issabrasil.org/> Acesso em: 28 Ago. 2011.

<http://dsconcursos.com.br/index.php?option=com_content&view=article&id=365:resumo-computacao-forense&catid=86:ti-seguranca-da-informacao&Itemid=129> Acesso em: 26 Ago. 2011.

MELO, Daniel. Pericia Contábil: aspectos técnicos, legais e éticos, FASB – Faculdade São Francisco Barreiras – Bahia, 2009 Disponível em:<http://www.fasb.edu.br/revista/index.php/ideia/article/viewFile/45/31> Acesso em: 19 Set. 2011.

<http://www.correiobraziliense.com.br/app/noticia/tecnologia/2011/10/12/interna_tecnologia,273670/fbi-prende-hacker-que-invadiu-contas-de-e-mail-de-celebridades.shtml> Acesso em: 10 Ago. 2011.

<http://www.terra.com.br/noticias/tecnologia/infograficos/hackers/hackers-06.htm> Acesso em: 15 Out. 2011.

<http://g1.globo.com/Noticias/Tecnologia/0,,MUL92187-6174,00.html> Acesso em: 12 Out. 2011.

<http://blogs.estadao.com.br/link/china-vai-aumentar-penalidades-de-hackers/ >Acesso em: 22 Set. 2011.

<http://www.clavis.com.br/empresa/sobre-institucional-historia-seguranca-da-informacao.php> Acesso em: 24 Out. 2011.

<http://gilbertomelo.com.br/jurisprudencias-e-noticias/90/832-pericia-forense-ganha-espaco-nas-empresas> Acesso em: 21 Out. 2011.

<http://www1.folha.uol.com.br/folha/informatica/ult124u712092.shtml> Acesso em: 28 Nov. 2011.

Luciano Cordova Tolentino Graduando (a) em Sistemas de Informação pela Escola de Tecnologia da Faculdade Projeção.

Paulo Augusto M. S. Mello Professor da Escola de Tecnologia da Faculdade Projeção e consultor em Tecnologia da Informação.

Wanessa da Silva Graduando (a) em Sistemas de Informação pela Escola de Tecnologia da Faculdade Projeção.