FORENSE COMPUTACIONAL : PROCEDIMENTOS E PADRÕES

Marcelo Abdalla dos Reis *
Instituto de Computação
Universidade Estadual de Campinas
13083-970 Campinas - SP
marcelo.reis@ic.unicamp.br

Paulo Lício de Geus
Instituto de Computação
Universidade Estadual de Campinas
13083-970 Campinas - SP
paulo@ic.unicamp.br

RESUMO

Nas últimas décadas a utilização de computadores tornou-se parte integrante da vida das pessoas. Infelizmente, aqueles que cometem crimes não estão alheios a essa revolução computacional. Desse modo, procedimentos válidos e confiáveis, aceitos pela comunidade científica relevante, que permitam recuperar dados de computadores envolvidos em atividades ilícitas e usá-los como indícios em investigações criminosas, estão se tornando fundamentais para as agências mantenedoras da lei. Este trabalho discute a necessidade de adoção de procedimentos e padrões para a realização de exames periciais em sistemas computacionais, apresentando uma visão geral da ciência forense computacional e propondo um modelo de padronização.

ABSTRACT

In the last few decades, the use of computers have become part of people's lifestyle. Unfortunately, those who commit crimes are not apart from this computer revolution. As a consequence, valid and reliable procedures, accepted by the relevant scientific community, which allow investigators to recover data from computers involved in illegal acts and use them as evidences in criminal investigations, are becoming fundamental to law enforcement agencies.

1 Introdução

Nas últimas décadas, a utilização de computadores tornou-se parte integrante da vida das pessoas. Transações bancárias e compras passaram a ser feitas pela Internet, informações diversas (desde simples correspondências pessoais até dados confidenciais) passaram a ser armazenadas e transmitidas de forma eletrônica, dispositivos digitais passaram a compor quase todo tipo de equipamento eletrônico (desde o rádio de pilhas até o mais avançado avião de passageiros), enfim, uma verdadeira revolução teve início.

Infelizmente, aqueles que cometem crimes não estão alheios a essa revolução computacional. Um número crescente de criminosos fazem uso de *pagers*, telefones celulares, computadores *laptop* e servidores de rede no curso de suas atividades ilícitas. Em alguns casos, os computadores provêem os meios para a consumação do crime. Por exemplo, a Internet pode ser usada para enviar uma ameaça de morte por corrêio eletrônico, para lançar ataques contra uma rede de computadores vulnerável, para disseminar vírus de computador, ou para transmitir imagens de pornografia infantil. Em outros casos, os computadores acabam se tornando dispositivos de armazenagem das evidências de um crime. Por exemplo, um traficante de drogas pode manter em seu computador pessoal uma listagem de quem lhe deve dinheiro, ou uma operação de lavagem de dinheiro pode reter falsos registros financeiros em um servidor de rede.

O aumento dramático em crimes relacionados com computadores requer que os organismos policiais invistam em novas técnicas de abordagem e combate aos crimes, através de treinamentos constantes e parcerias com entidades técnico-científicas, a fim de se entender como obter e utilizar evidências eletrônicas armazenadas em computadores. Registros eletrônicos como arquivos de log de redes de computadores, correspondências eletrônicas, arquivos de texto e de imagem provêem evidências importantes (às vezes essenciais) em casos de crimes.

Procedimentos válidos e confiáveis, aceitos pela comunidade científica relevante, que permitam recuperar dados de computadores envolvidos em atividades ilícitas e usá-los como indícios em investigações criminosas, estão se tornando fundamentais para as agências mantenedoras da lei. Tais procedimentos devem ser tecnologicamente robustos para garantir que toda informação probante seja descoberta. Além disso, eles devem ser legalmente defensáveis para garantir que nada na evidência original seja alterado e que nenhum dado possa ser adicionado ou removido do original [16].

A importância de procedimentos para se conduzir uma análise forense pode ser exemplificada através da citação de um caso que abalou a justiça americana, o julgamento do ex-jogador de futebol americano O. J. Simpson [27]. Simpson foi acusado de ter assassinado sua ex-mulher e um amigo dela, e na cena do crime foram coletadas diversas amos-

*O autor é financiado pela FAPESP

tras de sangue, que um exame de DNA comprovou serem de Simpson. A promotoria tinha uma identificação suficiente para condená-lo, entretanto, a defesa conseguiu anular todas as evidências de DNA e inocentá-lo. A estratégia da defesa foi de não contestar a validade do DNA como elemento probante, mas de levantar suspeitas nos procedimentos utilizados para se concluir que o DNA de Simpson estava nas amostras de sangue da cena do crime, provando que tais amostras poderiam ter sido contaminadas com o sangue de Simpson durante sua manipulação.

O caso de Simpson fez com que os institutos de criminalística norte-americanos revissem seus procedimentos, buscando corrigir falhas que pudessem levar a situações semelhantes. No âmbito computacional o problema é ainda maior. Um levantamento conduzido pelo Serviço Secreto dos Estados Unidos, em 1995, reportou que 70% das agências de investigação, que tinham laboratórios de forense computacional, estavam realizando seus trabalhos sem um manual de procedimentos escrito [16].

No Brasil, essa preocupação pode ser ilustrada pelos comentários do então Chefe do Setor de Crimes por Computador[1] (SECC) do Instituto Nacional de Criminalística (INC), André Machado Caricatti, durante um debate, em 15 de outubro de 1997, na Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados [23]. Caricatti falou da dificuldade por parte da Polícia Federal de responsabilizar e punir os que cometem crimes através da Internet, ressaltando, como principal preocupação, o estabelecimento de conceitos que ajudem a Polícia Federal a tomar providências legais contra aqueles que causam danos a terceiros.

Existem ainda outros agravantes no que diz respeito a crimes relacionados com computadores. A conectividade oferecida pela Internet permite que criminosos ajam em diferentes localidades com facilidade [17]. Consequentemente, um criminoso pode ser levado à justiça em um país, enquanto que as evidências digitais necessárias para processá-lo podem residir em outros.

Essa situação requer que todas as nações tenham a habilidade de coletar e preservar evidências digitais, não só para os interesses nacionais, mas também para uma potencial necessidade de outras nações. Nesse caso, os procedimentos utilizados para coletar, preservar e analisar evidências digitais devem ser coerentes com princípios legais e técnicos de comum acordo entre as nações, garantindo a legitimidade e aceitação das evidências [17].

Já existem esforços internacionais no sentido de desenvolver padrões para exames forenses em computadores e de prover estrutura para a forense computacional [17]. Entretanto, há muito por se fazer e o Brasil não deve ficar alheio a essas discussões, para que não se corra o risco de haver incompatibilidades futuras entre a legislação internacional e os interesses nacionais.

Este artigo propõe um estudo que visa o desenvolvimento de procedimentos e padrões para a realização de exames forenses em sistemas computacionais e está organizado como segue. A seção 2 apresenta uma breve explanação sobre a ciência forense computacional e na seção 3 é proposto um modelo de padronização para o desenvolvimento de procedimentos de análise forense em sistemas computacionais. Por fim, a seção 4 conclui este trabalho.

2 Forense Computacional

Forense computacional é o ramo da criminalística[2] 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 [16].

O propósito do exame forense é a extração de informações de qualquer vestígio[3] relacionado com o caso investigado, que permitam a formulação de colclusões acerca da infração [29].

A ciência forense tem produzido, ao longo dos anos, resultados que são considerados válidos e confiáveis. Embora não esteja previsto, na legislação processual brasileira, uma hierarquia de provas, acaba existindo uma prevalência da prova pericial no conjunto probante [29]. Tal preferência decorre do fato da prova pericial ser produzida a partir de fundamentação científica, não dependendo de interpretações subjetivas.

Para suportar os resultados de uma análise forense são necessários procedimentos e protocolos detalhados, documentados e revisados, aceitos pela comunidade científica relevante, que assegurem requisitos legais e técnicos à prova pericial [16]. Por exemplo, a identificação por meio de DNA é tida hoje como incontestável por dois motivos. Primeiro, devido a intensa pesquisa desenvolvida nessa área, os cientistas forenses de DNA demonstram estatisticamente que tal identificação é precisa. A outra razão é a consolidação de procedimentos robustos e defensáveis para a prática de exames forenses de DNA.

A forense computacional é uma área de pesquisa relativamente recente e são poucos os trabalhos

[1] Antigo Setor de Apuração de Crimes por Computador (SACC).

[2] Disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnico-científico, auxiliar e informativa das atividades policiais e judiciárias de investigação criminal, tendo por objeto o estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infrações penais e, ainda, à identificação dos autores respectivos [31].

[3] No universo da criminalística, vestígio é qualquer marca, fato, sinal ou material, que seja detectado em local onde haja sido praticado um fato delituoso. Enquanto que indício é o vestígio que, após devidamente analisado e interpretado, tem estabelecida sua inequívoca relação com o fato delituoso e com as pessoas com este relacionadas [31].

sobre esse assunto no Brasil. Entretanto, é crescente a necessidade de desenvolvimento nesse sentido, haja visto que a utilização de computadores em atividades criminosas é cada vez mais comum, tanto em crimes tradicionais (extorsão, roubos e tráfico de drogas, por exemplo) quanto nos chamados "crimes da Internet" (roubo de números de cartão de crédito de *sites* de comércio eletrônico, dados pessoais, segredos industriais, ataques de negação de serviço).

No exterior, em particular nos Estados Unidos, existem pesquisadores e profissionais dedicados a essa área, prestando serviços de investigação a empresas e órgãos do governo, como o FBI (Federal Bureau of Investigation). Porém, eles deparam-se com uma série de problemas que caracterizam temas em aberto para pesquisa, como por exemplo [9]: a capacidade limitada de correlacionar evidências de uma intrusão a uma rede de computadores; a dificuldade em organizar as evidências segundo uma linha de tempo (*timelining*); a necessidade da utilização da experiência do investigador durante os processos de extração e análise das evidências; e a inexistência de normas e procedimentos legalmente aceitos e avaliados pela comunidade científica para a realização de exames forenses em sistemas computacionais.

2.1 Fontes de Informação

A busca por indícios em um sistema computacional constitui-se de uma varredura minuciosa nas informações que nele residam, sejam dados em arquivos ou em memória, "deletados" ou não, cifrados ou possivelmente danificados. Tais indícios variam de acordo com o tipo de infração a que estão relacionados, determinando diferentes abordagens, no que diz respeito ao objetivo da busca, para o processo de análise forense.

Muitas vezes, o objetivo do exame forense é a busca de indícios que por si só caracterizam a infração, ou relacionam um suspeito ao ato ilícito (como, por exemplo, arquivos de imagens de pornografia infantil, mensagens eletrônicas com ameaças ou chantagens, arquivos com informações incriminatórias ou dados roubados). Outras vezes, os indícios são como "peças de um quebra-cabeça" (registros em arquivos de log e atributos de arquivos, por exemplo), precisando ser correlacionados para se concluir acerca da infração. Em alguns casos, ainda, a perícia objetiva responder alguns quesitos preestabelecidos, como, por exemplo, "descrever o conteúdo das mídias enviadas a exame", "determinar se o conteúdo de um determinado arquivo sofreu alterações".

Muitas são as fontes de informação para uma análise forense em um sistema computacional, podendo ser citadas as seguintes:

Sistema de arquivos

O sistema de arquivos representa a maior fonte de informação para o exame forense. Os arquivos de dados e executáveis são analisados para se determinar seu conteúdo e funcionalidade no sistema computacional. Os indícios podem ser encontrados através da busca por palavras-chave (como, por exemplo, datas, nomes, números de telefone e vocábulos específicos da linguagem criminal), imagens, dados específicos (registros em arquivos de log e informações roubadas, por exemplo) ou programas utilizados para práticas ilícitas (como *rootkits*[4] e *trojan horses*[5]).

Além disso, mudanças inesperadas em diretórios e arquivos, especialmente aqueles cujo acesso é normalmente restrito, podem caracterizar-se como indícios de uma infração. Tais mudanças podem incluir modificação, criação ou "deleção" de diretórios e arquivos (identificadas por alterações nos *MAC times*[6] dos arquivos ou por meio de assinaturas digitais). O que torna tais mudanças inesperadas pode depender de quem as concebeu, onde, quando, e como foram feitas.

Arquivos de log

Os arquivos de log representam um papel importante na análise do sistema de arquivos, pois permitem a reconstituição de fatos que ocorreram no sistema computacional.

Os arquivos de log variam de acordo com o sistema operacional, os aplicativos e serviços executando no sistema, e as configurações determinadas pelo administrador. Tais arquivos podem registrar, entre outras informações, as atividades dos usuários, dos processos e do sistema, as conexões de rede, as atividades da rede, e informações específicas dos aplicativos e serviços. Desse modo, os arquivos de log podem conter registros de atividades não usuais e inesperadas que ocorreram no sistema ou rede, caracterizando uma possível infração.

Espaços não utilizados no dispositivo de armazenagem

Os espaços no dispositivo de armazenagem não utilizados pelo sistema de arquivos podem conter indícios que o usuário tentou apagadar. A "deleção" de arquivos e diretórios não apaga os dados do dispositivo de armazenagem, apenas disponibiliza o espaço ocupado para ser sobrescrito por novos arquivos.

Esses espaços podem ser caracterizados por espaços não alocados dentro do sistema de arquivos, espaços alocados a arquivos mas não totalmente utilizados (os chamados *file slacks*[7]) e áreas do disposi-

[4] Conjunto de ferramentas, utilizadas por usuários mal intensionados, para conseguir privilégios de *root* em um sistema alvo e esconder suas atividades.

[5] Programas que contêm código malicioso, mas que parecem ser inofensivos.

[6] Atributos dos arquivos que registram os últimos tempos de modificação de conteúdo, acesso e alteração de atributos.

[7] Os *file slacks* ocorrem pelo fato do sistema de arquivos alocar blocos de tamanho fixo. Por exemplo, um arquivo com tamanho de 2460 bytes, em um sistema de arquivos com tamanho de bloco de 1024 bytes, ocupa três blocos de

tivo de armazenagem que não constituem uma partição de disco ou que não contém um sistema de arquivos (é possível ler e escrever dados no dispositivo de armazenagem sem a abstração de arquivos, o que é chamado de *raw I/O*).

Arquivos temporários

Alguns programas de processamento de texto e de banco de dados criam arquivos temporários durante sua execução, que são normalmente apagados automaticamente ao final da sessão de trabalho. Tais arquivos podem conter indícios e são particularmente interessantes quando o arquivo original foi cifrado ou nunca foi salvo no dispositivo de armazenagem [9].

Área de *swap*

A área de *swap* é utilizada pelo gerenciador de memória do sistema operacional como uma grande área de armazenamento temporário, permitindo que processos sejam momentaneamente descarregados da memória principal, liberando espaço para a execução de outros [2, 3]. A área de *swap* pode ser tanto um arquivo quanto uma partição inteira do disco, podendo conter fragmentos de dados ou até mesmo um arquivo texto completo.

Setor de *boot*

O setor de *boot* de um computador contém informações relativas aos programas que são carregados quando o computador é inicializado [1, 9]. Se tais informações forem modificadas, é possível carregar qualquer programa durante a inicialização do computador.

Memória

A memória principal contém todo tipo de informação volátil, como, por exemplo, informações dos processos que estão em execução, dados que estão sendo manipulados e muitas vezes ainda não foram salvos no disco e informações do sistema operacional. Tais informações podem ser acessadas por meio de *dumps* da memória ou pela geração de *core files*[8].

Periféricos

Muitos dispositivos como *modems*, *pagers*, aparelhos de fax e impressoras, contêm memórias que podem ser acessadas e salvas [9]. Além disso, dispositivos não autorizados podem ter sido implantados no sistema computacional, possibilitando a execução da infração.

Comportamento de processos

Cada processo executa em um ambiente com privilégios específicos que determinam quais recursos do sistema, programas e arquivos de dados podem ser acessados, e de que modo. O comportamento de um processo é representado pelas operações que ele executa, pela maneira como tais operações são realizadas, e pelos recursos do sistema que o processo utiliza.

Um invasor pode desvirtuar a execução de um programa ou serviço, causando sua falência, ou fazendo com que ele opere de maneira inesperada ao administrador ou usuário (acessando informações não autorizadas ou consumindo recursos excessivos, por exemplo).

alocação, desperdiçando os últimos 612 bytes alocados.

[8] Arquivos com dados e informações da memória utilizada pelos processos.

3 Modelo de Padronização

O desenvolvimento de procedimentos e padrões para exames periciais em sistemas computacionais deve ser regido por aspectos de ordem legal e técnica. Os aspectos técnicos, por sua vez, devem ser regidos pelos de ordem legal, garantindo que os procedimentos periciais sejam defensáveis.

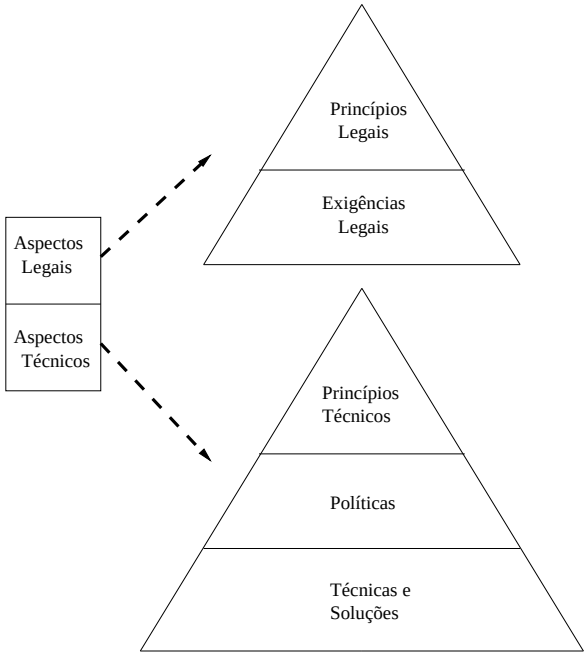

Figura 1: Modelo de padronização.

Na figura 1, é ilustrado um modelo de padronização, proposto pelos autores deste artigo, para o desenvolvimento de procedimentos de análise forense em sistemas computacionais. O modelo proposto é uma estrutura hierárquica de duas classes multiníveis relacionadas entre si:

- A classe dos aspectos legais, no topo da hierarquia, onde encontram-se as exigências legais a que devem estar sujeitos os procedimentos periciais;
- E a classe dos aspectos técnicos, regida pela classe anterior, cujos componentes referem-se às questões práticas da área computacional.

Esse modelo é baseado no modelo apresentado em [16], distinguindo-se pela inclusão da classe dos aspectos legais, o que permite modelar a necessidade de aceitação legal dos procedimentos periciais.

O detalhamento de cada classe do modelo proposto é apresentado como segue.

Classe dos Aspectos Legais

Os aspectos legais constituem-se das formalidades e enquadramentos judiciais a que estão sujeitos os peritos e a função pericial. Tais exigências legais estão dispostas no Código de Processo Penal Brasileiro, no entanto, a legislação processual data de 1941 e, atualmente, o universo de perícias que nela deveria estar regulamentado é bem maior [29].

As exigências legais devem obedecer princípios que permitam a utilização de evidências digitais por jurisdições com diferentes legislações. Como exemplos de tais princípios podem ser citados os seguintes [29, 31, 28]:

- a função pericial dever ser exercida por pessoa portadora de nível superior, forensicamente capacitada, com habilitação técnica relacionada à natureza do exame e sem antecedentes que levantem suspeitas acerca de seu caráter e ética;
- o exame pericial deve produzir um laudo pericial segundo algum modelo preestabelecido;
- o perito deve ser judicialmente responsável pelos resultados da perícia e pelas evidências, enquanto em sua posse;
- os casos de suspeição dos peritos devem ser predispostos;
- o exame pericial deve ser realizado por mais de um perito, permitindo conclusões livres de interpretações pessoais;
- condições de trabalho adequadas devem ser garantidas ao perito, especialmente na disponibilidade de equipamentos e materiais necessários ao exame pericial, garantindo a realização de um trabalho eficaz e eficiente;
- o perito deve lastrear suas assertivas e conclusões com justificativas científicas, de modo que haja, do ponto de vista científico, uma única possibilidade para se chegar a tais afirmações;
- o exame pericial deve ser obrigatório caso haja vestígios a serem analisados;
- o exame pericial deve preservar os vestígios de modo a permitir a realização de nova perícia;
- o estado original dos vestígios deve ser mantido até a chegada dos peritos. Qualquer alteração deve ser relatada;
- o resultado do exame pericial deve ser o mais elucidativo possível, sendo permitida a utilização de fotografias, desenhos ou esquemas;

Aspectos Técnicos

Os aspectos técnicos referem-se aos requisitos práticos e condutas para a execução do exame propriamente dito. Tais aspectos são organizados como segue.

_ Princípios Técnicos

Conceitos básicos que sempre se aplicam a todos os exames. Devem garantir requisitos mínimos às evidências, como confiabilidade, integridade e durabilidade. Dentre alguns desses princípios podem ser citados [9, 17]:

- as ações tomadas durante o exame pericial não devem alterar as evidências;
- a cadeia de custódia das evidências deve ser montada, relatando o nome da pessoa que está de posse da evidência, data, hora e atividades executadas;
- cópias dos vestígios originais, armazenados eletronicamente, devem ser produzidas, e sempre que possível os exames devem ser realizados nas cópias;
- as cópias dos vestígios digitais devem ser autenticadas por meio de assinaturas criptográficas;
- não se deve confiar no sistema analisado, pois este pode estar adulterado;
- todas as suposições que apareçam durante o exame devem ser relatadas;
- mídias esterelizadas, devidamente preparadas e forensicamente verificadas, devem ser utilizadas;
- tudo deve ser documentado, desde os exames realizados até a descrição dos vestígios analisados e dos indícios encontrados, permitindo a replicação da análise;
- precauções com escritas não autorizadas, por consequência de vírus de computador ou esquemas de defesa do tipo *booby trap*[9], devem ser tomadas;
- as ferramentas e técnicas de análise devem ser conhecidas a fundo, de modo a se saber todos os seus efeitos e implicações no sistema analisado;
- cuidado e atenção devem ser tomados com relação a unidades de medida e aproximações matemáticas, para evitar que informações nos dispositivos de armazenagem sejam "esquecidas" durante a análise;

[9] Armadilhas implantadas por usuários mal intensionados que podem apagar os indícios de suas atividades, ou dificultar o processo de análise.

- todos os mecanismos que a ciência dispõem devem ser utilizados para acessar informações "deletadas", travadas, escondidas, protegidas por senhas ou cifradas. Tais mecanismos devem ser relatados;
- os resultados e dados da análise devem ser mantidos em dispositivos de armazenagem confiáveis e protegidos do acesso de estranhos (blocos de notas e computadores *offline*, por exemplo);
- os indícios devem ser procurados em todas as fontes possíveis e relevantes, observando a ordem de volatilidade de tais fontes;
- todas as ferramentas utilizadas no exame pericial devem ser licenciadas ou autorizadas para o uso do perito;
- o exame completo do sistema computacional pode não ser autorizado, possível ou necessário. Os motivos para tal devem ser relatados;

_ Políticas

Guia prático aplicado aos exames periciais, determinando como eles são planejados, executados, monitorados, gravados e relatados para assegurar a qualidade e integridade dos resultados obtidos. É composto por instruções passo a passo aplicáveis à maioria dos exames, podendo variar de acordo com particularidades do sistema computacional examinado e do tipo de análise executada. Um esboço desse guia é apresentado como segue [9, 11, 12, 15, 18].

- *Passo 0*: Determinar a melhor abordagem para o exame, identificando todas as atividades que precisarão ser executadas;
- *Passo 1*: Preparar o sistema de análise, provisionando a melhor configuração de *hardware* e *software*, devidamente testados e forensicamente esterelizados, para a realização dos exames (em alguns casos será necessário recriar uma configuração específica, como, por exemplo, uma topologia de rede);
- *Passo 2*: Estabilizar a condição inicial do sistema computacional a ser examinado, de modo a preservar o máximo de vestígios possíveis e proteger dados e sistemas não comprometidos. O sistema computacional examinado deve ser minuciosamente descrito em sua condição inicial (configurações de *hardware* e *software*, processos em execução, conexões de rede, corretude da data e hora do sistema, por exemplo). Algumas questões devem ser avaliadas, como, por exemplo, o desligamento do sistema (em que momento deve ser feito e de que maneira), a manutenção do sistema *online* ou *offline*, a necessidade de se capturar tráfego de rede e informações detalhadas de processos em execução (geração de *core files*) e a finalização de processos que possam apagar vestígios (*booby traps* e *rootkits*, por exemplo);
- *Passo 3*: Proceder à cópia das informações armazenadas eletronicamente no sistema computacional. A cópia deve conter toda a informação, em seu estado original, e deve ser autenticada;
- *Passo 4*: Coletar o máximo de informações pertinentes na ordem de volatilidade das mesmas;
- *Passo 5*: Analisar cada informação separadamente em busca de indícios, e depois de maneira correlata.
- *Passo 6*: Tentar estabelecer relações entre os indícios encontrados (indícios computacionais ou não);
- *Passo 7*: Elaborar o laudo pericial, reunindo todas as informações resultantes do exame;

_ Técnicas e Soluções

Soluções de *hardware* e *software* específicas para determinadas atividades executadas durante o exame. Constituem-se de instruções detalhadas que descrevem o uso de técnicas e ferramentas empregadas na consumação das atividades. Um exemplo de solução é apresentado como segue.

Solução para efetuar a cópia do disco rígido, com interface IDE, de um computador apreendido para o sistema de análise (montado em um *Intel Pentium III* equipado com sistema operacional *Red Hat Linux 7.1*):

- *Passo 1*: Anote as informações que possivelmente venham impressas na superfície externa do disco, como sua geometria, além da posição original dos *jumpers*;
- *Passo 2*: Instale o disco no sistema de análise em uma das portas IDE secundárias e ligue o sistema. Para evitar danificar o disco com possíveis conflitos mestre/escravo na controladora IDE, instale o disco como único dispositivo na interface IDE secundária. Será considerado, nos passos seguintes, que o disco examinado é acessível no sistema de análise pelo dispositivo de bloco */dev/hdc* (correspondente à interface IDE secundária mestre);
- *Passo 3*: Faça a detecção do disco na BIOS do sistema de análise. Verifique e anote a geometria detectada;
- *Passo 4*: Gere a assinatura MD5[10] das informações do disco copiado, através do comando *dd if=/dev/hdc | md5sum -b*;

[10] Soma verificadora de qualidade criptográfica.

- *Passo 5*: Faça a cópia do disco para o sistema de análise usando o comando *dd if=/dev/hdc of=arquivo*, onde *arquivo* é o nome do arquivo que irá conter a cópia (é conveniente nomeá-lo de maneira sugestiva e armazená-lo em uma hierarquia de diretórios referente ao caso em questão, de preferência em uma partição do sistema de análise reservada);

- *Passo 6*: Gere a assinatura MD5 do arquivo que contém a cópia do disco, através do comando *dd if=arquivo | md5sum -b*. Compare com a assinatura MD5 do disco gerada no *Passo 4*;

4 Conclusão

A criminalística, por ser uma ciência que se utiliza do conhecimento de outras ciências [29], necessita manter-se atualizada em relação aos desenvolvimentos técnico-científicos. A forense computacional, por ser uma disciplina forense bastante recente e relacionada a uma das áreas científicas que mais evolui atualmente, requer atenção especial. Além disso, a crescente utilização de computadores em atividades criminosas fundamenta tal necessidade de desenvolvimento, no sentido de se entender como obter e utilizar evidências digitais no amparo à justiça.

Segundo o perito criminal Alberi Espindula[11], que possui um currículo expressivo na área da ciência criminal, a criminalística carece de algumas definições e metodologias mais sofisticadas para aplicação no dia-a-dia da perícia. Espindula ressalta a falta de apoio das instituições em relação à pesquisa científica aplicada à criminalística, no sentido de se chegar a resultados satisfatórios na escolha dos melhores procedimentos e metodologias [30].

O estudo proposto neste artigo representa um esforço no sentido de suprir essa necessidade de desenvolvimento científico. Entretando, muitas são as dificuldades a serem endereçadas ao longo desse estudo, podendo ser citadas questões como:

- a dificuldade em se documentar tudo na forma de procedimentos operacionais, devido à grande variedade de exames que podem ser requisitados, e a variantes impostas pela diversidade de tecnologias, que evoluem constantemente. Nesse sentido, a característica hierárquica do modelo apresentado na seção 3 permite abordar tal dificuldade;

- o respeito à privacidade no processo de análise das informações, dentre as quais podem residir documentos que são comunicações entre o suspeito e seu advogado, padre ou cônjuge. Entretanto, na maioria das vezes, tais informações só são identificadas como privativas depois de acessadas. Além disso, as evidências podem ser "camufladas" dentre essas informações sigilosas;

- a falta de ferramentas para análise e correlação das evidências. Tais processos dependem totalmente da experiência do investigador e despendem muito tempo;

- o montante de informação a ser analisada cresce à medida que os dispositivos de armazenagem têm sua capacidade aumentada. A realização de um exame completo e eficiente torna-se um desafio;

- a dificuldade no acesso a informações cifradas ou protegidas por senhas;

- a necessidade de adoção de políticas de segurança que viabilizem exames forenses mais eficientes e precisos, como, por exemplo, a utilização de esquemas de log mais detalhados e insuscetíveis a adulterações;

[11] No currículo de Alberi Espindula destacam-se os cargos de Perito Criminal Oficial do Distrito Federal, ex-Chefe da Seção de Crimes contra a Pessoa e ex-Diretor da Divisão de Perícias Externas do Instituto de Criminalística do DF, ex-Presidente da Associação Brasileira de Criminalística e Professor nas Academias de Polícia do DF, MA, BA e ANP/DPF

Referências

[1] Stallings, W. *Computer Organization and Architecture*, 5th Edition.

[2] Galvin, S. *Operating System Concepts*, 5th Edition.

[3] McKusick, M., Bostic, K., Karels, M. (1996) *The Design and Implementation of the 4.4 BSD Operating System.* Addison-Wesley.

[4] Nemeth, E., Snyder, G. (2000). *UNIX System Administration Handbook* , 3rd Edition. Pearson.

[5] Stevens, R. W. (1994). *TCP/IP Illustrated, Volume I: The Protocols.* Addison-Wesley: Reading, MA.

[6] Garfinkel, S. and Spafford, G. (1996). *Practical Unix and Internet Security*, 2nd Edition. O'Reilly and Associates, Inc.

[7] Farmer, D., and Venema, W. (1993). *Improving the security of your site by breaking into it.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fish.com/security/admin-guide-to-cracking.html>.

[8] Spafford, G., and Weeber, S. (1992). *Software Forensics: Can We Track Code to its Authors?* Purdue Technical Report CSD-TR 92-010.

[9] Hosmer, C., Feldman, J., and Giordano, J. (2000). *Advancing Crime Scene Computer Forensic Techniques.* WetStone Technologies Inc. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://wetstonetech.com/crime.htm>.

[10] Robbins, J. (2000). *An explanation of Computer Forensics.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://computerforensics.net/forensics.htm>.

[11] Farmer, D., and Venema, W. (1999). *Computer Forensics Analysis Class Handouts.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fish.com/forensics/class.html>.

[12] Firth, R., Ford, G., Fraser, B., et al. (1997). *Detecting Signs of Intrusion.* Security Improvement Module, CERT Coordination Center. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.cert.org/security-improvement/modules/m09.html>.

[13] Kochmar, J., Allen, J., Alberts, C., et al. (1998). *Preparing to Detect Signs of Intrusion.* Security Improvement Module, CERT Coordination Center.

[14] Casey, E. (2000). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.* Academic Press.

[15] *Evidence Examinations - Computer Examinations.* (1999). Handbook of Forensic Services, U.S. Department of Justice, FBI. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fbi.gov/hq/handbook/examscmp.htm>.

[16] Noblett, M., Pollitt, M., and Presley, L. (2000). *Recovering and Examining Computer Forensic Evidence.* Forensic Science Communications, October 2000, Volume 2, Number 4. U.S. Department of Justice, FBI. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/computer.htm>.

[17] Scientific Working Group on Digital Evidence, International Organization on Digital Evidence (1999). *Digital Evidence: Standards and Principles.* Forensic Science Communications, April 2000, Volume 2, Number 2. U.S. Department of Justice, FBI. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm>.

[18] Dittrich, D. *Basic Steps in Forensic Analysis of Unix Systems.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://staff.washington.edu/dttrich/misc/forensics>.

[19] Venema, W., Farmer, D. (2000). *The Coroner's Toolkit.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.fish.com/tct>.

[20] Farmer, D., Venema, W. (2000). *Forensic Computer Analysis: An Introduction.* Dr. Dobb's Journal, September 2000. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.ddj.com/articles/2000/0009/0009f/0009f.htm>.

[21] Farmer, D. (2000). *What Are MACtimes ?* Dr. Dobb's Journal, October 2000. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.ddj.com/articles/2000/0010/0010f/0010f.htm>.

[22] Venema, W. (2000). *Strangers in the Night.* Dr. Dobb's Journal, November 2000. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.ddj.com/articles/2000/0011/0011g/0011g.htm>.

[23] *Crimes Cometidos nas Redes Integradas de Computadores.* (1997). Debate na Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados. Comitê Gestor da Internet no Brasil. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://cg4.cg.org.br/infoteca/debates/debate1.htm>.

[24] *NBSO: NIC BR Security Office.* (2001). [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.nic.br/nbso.html>.

[25] *Grupo de Trabalho de Segurança de Redes do Comitê Gestor da Internet no Brasil.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://cg.org.br/grupo/grupos.htm#Grupo>.

[26] Reis, Marcelo A., Oliveira, F., Geus, P. L., Guimarães, C. (2001). *Forense Computacional: Aspectos Legais e Padronização.* Anais do Workshop em Segurança de Sistemas Computacionais - WSeg2001, IX Simpósio de Computação Tolerante a Falhas - SCTF2001, Florianópolis, SC, 5 - 6/03/2001, pp 80 - 85.

[27] Cable News Network, Inc. (1995). *CNN - O. J. Simpson Trial.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.cnn.com/US/OJ/index.html>.

[28] Kerr, O. S. (2001). *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.* Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, United States Department of Justice. [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.cybercrime.gov/searchmanual.htm>.

[29] Espindula, A. *A Função Pericial do Estado.* [on line]. [citado em abril de 2001]. Disponível em World Wide Web: <URL:http://www.apcf.org.br>.

[30] Espindula, A. *Técnicas Criminalísticas para Conclusão de Laudo Pericial.* [on line]. [citado em junho de 2001]. Disponível em World Wide Web: <URL:http://www.tba.com.br/pages/espindula>.

[31] Tochetto, D., Galante, H., Zarzuela, J., et al. (1995). *Tratado de Perícias Criminalísticas.* Editora Sragra-DC Luzzatto, 1^a Edição.