Computação Forense e a Perícia Criminal

A Informática a Serviço da Justiça

Marcio Pereira Machado, mpm.marcio@yahoo.com.br, Departamento de Polícia Federal.
Pedro Monteiro da Silva Eleutério, pedro@eleuterio.com, Departamento de Polícia Federal.

Este artigo tem objetivo de apresentar uma profissão pouco conhecida no meio acadêmico da computação: o Perito Criminal da área de Informática. Além disso, divulgar a Computação Forense, apresentando alguns conceitos, os tipos de exames mais comuns e as fases executadas pelo Perito Criminal durante os exames periciais.

Os crimes envolvendo equipamentos computacionais vêm crescendo, seja pelas facilidades disponibilizadas por essa tecnologia, pela velocidade da comunicação, e também pela própria especialização dos hackers. Por envolver questões técnicas bem específicas, a justiça necessita de um profissional bem treinado, que seja capaz de auxiliar a apuração de crimes envolvendo a utilização de computadores.

O Código de Processo Penal (CPP) determina em seu art. 158 que "Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.". Dessa forma, surge a necessidade de um profissional qualificado, que examine vestígios e produza laudos de interesse à justiça na apuração de um delito, conforme definidos nos *caputs* dos artigos 159 e 160 do CPP, que dizem, respectivamente: "O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior." e "Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados". No caso específico da área da computação, quem realiza esse trabalho de identificar as evidências digitais de delitos e crimes de forma oficial no âmbito criminal é o Perito Criminal em Informática. Entretanto, diversos outros profissionais podem ter a necessidade de realizar exames em computação. São eles: peritos particulares, auditores de sistemas, profissionais de TI e outros. Além disso, juízes, advogados, delegados, promotores e demais profissionais da área de direito também devem conhecer como evidências e provas digitais devem ser corretamente coletadas, apuradas e apresentadas em juízo. Sendo assim, a Computação Forense tem o objetivo principal de determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à área de informática, identificando e processando as evidências digitais em provas materiais de crime, com a utilização de métodos técnico-científicos, conferindo-lhes validade probatória em juízo.

A Carreira de Perito Criminal

Para se tornar um Perito Criminal de carreira é necessário ter formação de nível superior em área específica, conforme prevê a Lei 12.030/09, e é obrigatória a aprovação em concurso público, que pode ser de provas ou de provas e títulos. Os Peritos Criminais são vinculados às Polícias Judiciárias (Civil ou Federal) ou às Polícias Científicas, que foram criadas em alguns Estados no intuito de dar autonomia administrativa e criar certa desvinculação da perícia em relação à polícia.

O concurso público geralmente é composto de duas etapas. A primeira etapa consiste de cinco fases: prova escrita, avaliação psicológica, prova de capacidade física, exames médicos e investigação social (realizada pelas próprias instituições). A segunda etapa consiste de um curso de formação profissional em que o candidato é treinado pela própria Instituição para exercer essa função. Todas as fases são eliminatórias.

A remuneração desses servidores públicos varia em cada Estado da Federação, além da própria União. Atualmente, um Perito Criminal da Polícia Federal tem uma remuneração inicial de R$13.368,68. Mesma remuneração tem os Peritos Criminais da Polícia do Distrito Federal. No entanto, a realidade nos demais estados é diferente. A média gira em torno de R$5.000,00.

Esta é uma publicação eletrônica da Sociedade Brasileira de Computação – SBC. Qualquer opinião pessoal não pode ser atribuída como da SBC. A responsabilidade sobre o seu conteúdo e a sua autoria é inteiramente dos autores de cada artigo.

Concurso da Polícia Federal

Na Polícia Federal, no último concurso público nacional, realizado em 2004, foram oferecidas inicialmente 84 vagas para a área de informática e foram registradas 9.032 inscrições, gerando uma concorrência de 107,52 candidatos/vaga. A prova escrita foi composta de conhecimentos básicos e específicos. Vale lembrar que existem diversas especialidades entre os Peritos Criminais Federais e os concursos são divididos por área de formação. Algumas delas são: Contabilidade, Informática, Engenharia Civil, Engenharia Elétrica, Medicina, Odontologia, Veterinária, Farmácia, Química, Biologia, entre outras.

A prova de conhecimentos básicos, comum a todas as áreas de perícias, exigiu as seguintes disciplinas: língua portuguesa, conhecimentos de informática, atualidades, raciocínio lógico e Noções de Direito.

Já a prova específica da área de informática abordou os seguintes tópicos: Fundamentos de Computação, Desenvolvimento de Sistemas, Reengenharia de Sistemas, Linguagens de Programação, Redes de Comunicação de Dados, Segurança da Informação, Criptografia e Sistemas Operacionais.

A Coleta das Provas

O trabalho dos Peritos Criminais da área de Informática é pautado em doutrinas e procedimentos técnico-científicos, que visam à preservação e integridade da prova. Geralmente, o trabalho inicia-se com o cumprimento de mandados de busca e apreensão ou exames em locais de crime. Em ambos os casos, cabe ao Perito a identificação e posterior coleta das provas, tomando-se o extremo cuidado com a preservação e a cadeia de custódia, que é o processo de garantia de proteção à prova, cujo objetivo é assegurar sua idoneidade, a fim de evitar questionamentos quanto à sua origem ou seu estado inicial. Para isso, devem ser registrados todos os caminhos percorridos pela prova durante a persecução penal, ou seja, desde a sua coleta até o trânsito em julgado da ação.

No caso específico da computação, a manipulação dos dados contidos em mídias de armazenamento computacional deve ser realizada com toda atenção possível, pois a prova não pode ter seu estado inicial alterado, ou seja, nenhum bit pode ser modificado. Isso garante a validade da prova em juízo. Para isso, o Perito deve sempre utilizar equipamentos e softwares forenses. Para se ter uma ideia da sensibilidade das evidências digitais, apenas ao ligar um computador e aguardar seu sistema operacional ser inicializado, dados contidos no disco rígido já são alterados, mesmo sem qualquer intervenção direta do usuário.

Exames Periciais em Mídias de Armazenamento Computacional

São os exames mais comuns realizados pelos Peritos Criminais da área de Informática e têm o objetivo principal de identificar as evidências digitais contidas em discos rígidos, *pen drives*, mídias ópticas, cartões de memória, entre outros dispositivos de armazenamento. Durante sua execução, quatro fases principais devem ser seguidas, que vão desde o recebimento do material até a conclusão do laudo. São elas: preservação; extração; análise e formalização.

Fase 1 – Preservação. Fase que consiste em garantir que as informações armazenadas no material examinado jamais sejam alteradas. Por isso, os exames devem, sempre que possível, ser realizados em cópias fiéis obtidas a partir do material original, utilizando técnicas de espelhamento ou de imagem. Durante a cópia, a fim de registrar o conteúdo presente no material examinado, é recomendável a aplicação de funções hash sobre partes e/ou todo o conteúdo do dispositivo de armazenamento. Tal procedimento visa garantir a integridade das evidências contidas e evitar questionamentos jurídicos futuros.

Fase 2 – Extração. Consiste em recuperar as informações contidas na cópia dos dados provenientes da fase de preservação. Nesta fase, deve ser realizada a recuperação dos arquivos eventualmente apagados, uma vez que, ao apagar um arquivo de um dispositivo, o sistema operacional não

sobrescreve todo o conteúdo ocupado por esse arquivo com zeros e/ou uns. Ele apenas tem um controle de quais partes do disco rígido estão livres e quais estão ocupadas. Assim, técnicas apropriadas devem ser aplicadas no conteúdo da mídia, fazendo com que tais arquivos sejam acessíveis para análise por parte dos Peritos. Outra técnica bastante utilizada no meio forense é o Data Carving, que consiste na busca de arquivos apagados com formatos conhecidos a partir de suas assinaturas.

Fase 3 – Análise. Consiste no exame das informações extraídas, a fim de identificar evidências digitais presentes no material examinado, que tenham relação com o delito investigado. Nesta fase, os Peritos devem ser muito criteriosos, evitando-se, assim, que algum conteúdo que possa estar relacionado com os quesitos formulados seja desconsiderado. É a principal fase do exame pericial e a que exige maior esforço, cuidado e capacidade técnica do Perito. Atenção especial deve ser dada a arquivos com senha, criptografados e esteganografados, além do exame de possíveis sistemas e programas existentes no dispositivo examinado.

Fase 4 – Formalização. Consiste na elaboração do laudo pelo Perito, apontando o resultado e apresentando as evidências digitais encontradas nos materiais examinados. No laudo devem constar os principais procedimentos realizados, incluindo as técnicas utilizadas para preservar, extrair e analisar o conteúdo das mídias digitais.

Pedofilia, a Exploração Sexual de Crianças e a Legislação

Um dos crimes mais comuns no âmbito da Computação Forense é a exploração sexual de crianças, caracterizada pelo uso de equipamentos computacionais para produção, edição, visualização e divulgação de imagens e vídeos contendo pornografia infanto-juvenil pela Internet.

Segundo Delton Croce, pedofilia é o "desvio sexual caracterizado pela atração por crianças ou adolescentes sexualmente imaturos, com os quais os portadores dão vazão ao erotismo pela prática de obscenidades ou de atos libidinosos". Sendo assim, pedofilia é uma doença e/ou desvio aplicado aos seres humanos e não pode ser confundido com pornografia infanto-juvenil. Logo, é incorreto dizer que um arquivo de vídeo é pedófilo - esse é um erro bastante comum na mídia e nos noticiários.

Até 25 de novembro de 2008, a legislação brasileira não considerava crime a posse de arquivos de pornografia envolvendo crianças ou adolescentes. Apesar de o compartilhamento, a produção e a divulgação, entre outras ações, já estarem contempladas pela legislação, a posse ainda não tinha previsão legal. Tal mudança, realizada pela lei 11.829, mostra uma preocupação da sociedade com o assunto e a mobilização do governo em combater esse tipo de delito.

A produção e propagação de conteúdo digital ilegal, especialmente imagens e vídeos envolvendo pornografia infanto-juvenil, tem crescido nos últimos tempos. Combinada com a rápida evolução dos computadores e a popularização da Internet, a produção e o consequente compartilhamento de arquivos ilegais entre pessoas de todo mundo ocorre de maneira frequente, principalmente por meio da *World Wide Web* (WWW), das redes *peer-to-peer* (P2P), de emails e dos serviços de mensagens instantâneas, como *Messenger* e *Skype*.

Com o intuito de reprimir e desencorajar a prática desse tipo de crime, as polícias de quase todo o mundo, inclusive a Polícia Federal do Brasil, têm realizado uma série de operações, visando à identificação de pessoas que tenham, principalmente, compartilhado arquivos contendo pornografia infanto-juvenil por meio da Internet. A partir da identificação dessas pessoas, em alguns casos, é possível identificar também o produtor dos arquivos de imagens/vídeos, bem como a identificação e posterior recuperação psicológica da própria vítima (criança/adolescente), conforme mostra um trabalho anteriormente publicado pelos autores (Recurso nº 4).

As operações da Polícia Federal contam com a participação dos Peritos Criminais Federais. O Perito atua desde a fase de investigação, quando acontece o monitoramento do tráfego de Internet para a

identificação dos responsáveis pela transmissão do conteúdo, até a elaboração dos laudos periciais nos equipamentos apreendidos no dia da deflagração da operação. Nesse dia, inclusive, pode compor equipes de busca e apreensão para orientar quanto à seleção do material a ser apreendido, bem como pode realizar alguns procedimentos no próprio local, a fim de auxiliar a autoridade policial na condução de uma prisão em flagrante delito. Isso acontece quando é identificado que o responsável está transmitindo ou tem a posse de algum arquivo contendo pornografia infanto-juvenil.

Outros Exames Periciais

Além dos exames periciais anteriormente descritos, um Perito Criminal da área de Informática pode realizar uma série de outros exames. Os mais comuns estão listados abaixo:

a) Exames em Mensagens Eletrônicas (emails): consistem na identificação do remetente e rastreamento do email, a partir da análise das propriedades das mensagens eletrônicas, a fim de identificar hora, data, endereço IP e outras informações.

b) Exames em Sites da Internet: consistem principalmente na verificação e cópia de conteúdo existente na Internet, em sites e servidores remotos dos mais variados serviços. Além disso, trata-se da investigação do responsável por um domínio de um site, servidor e/ou endereço IP.

c) Exames em Aparelhos de Telefone Celular: consistem na extração dos dados desses aparelhos, a fim de recuperar e formalizar as informações armazenadas em suas memórias (lista de contatos, ligações, fotos, mensagens, dentre outros), de acordo com a necessidade de cada caso.

d) Exames em Caça-Níqueis e Máquinas de Jogos de Azar: consistem na verificação e comprovação da existência da prática do jogo de azar, marcado pela ausência de habilidade do jogador, como caça-níqueis e vídeo bingo.

e) Análise de Vírus e *Malwares* (*Malicious Softwares*): são exames que tem por objetivo identificar o comportamento de programas maliciosos diversos, a fim de encontrar os responsáveis pela tentativa de fraude eletrônica.

Considerações Finais

A Computação Forense é uma área que envolve a análise e coleta de vestígios e evidências digitais em equipamentos computacionais envolvidos em procedimentos ilícitos e crimes de qualquer natureza. Para aplicação das técnicas de forma correta é necessária a atuação de um profissional bem qualificado: o Perito Criminal.

Atualmente, trata-se de uma área pouco explorada no meio acadêmico e que tem várias portas abertas para pesquisas. Há muito espaço para quem deseja desenvolver projetos. No ramo profissional, além dos Peritos Criminais concursados, existem diversos profissionais que se especializam na área e são necessários em empresas de TI e na segurança da informação. Sendo assim, é uma área de atuação profissional bastante promissora para os formados em Computação.

Recursos

CROCE, D. *Manual de Medicina Legal*. São Paulo: Saraiva, 1995.

EDITAL N.º 24/2004 - DGP/DPF - NACIONAL, DE 15 DE JULHO DE 2004.

ELEUTÉRIO, PMS, & MACHADO, MP. (Jan de 2011). *Desvendando a Computação Forense*. 1.ed. São Paulo: Novatec, 2011. ISBN 978-85-7522-260-7, 200p.

ELEUTÉRIO, PMS., & MACHADO, MP. (Set de 2009). Identificação de autoria e materialidade em crimes de abuso sexual de criança/adolescente a partir da análise de arquivos multimídia. *Proceedings of The Fourth International Conference of Forensic Computer Science (ICoFCS 2009)* , pp. 114-121.

Sobre os Autores

Marcio Pereira Machado é bacharel em Ciência da Computação pela Universidade Federal do Espírito Santo (UFES). Desde 2005, é Perito Criminal Federal do Departamento de Polícia Federal. Autor do livro Desvendando a Computação Forense, da Novatec Editora. Antes de se tornar Perito Criminal Federal, atuou como desenvolvedor de sistemas de automação bancária.

Pedro Monteiro da Silva Eleutério é mestre em Ciência da Computação, área de Hipermídia, pela Universidade de São Paulo (USP) e Engenheiro de Computação pela Universidade Federal de São Carlos (UFSCar). Desde 2006, é Perito Criminal Federal do Departamento de Polícia Federal. Autor do livro Desvendando a Computação Forense, da Novatec Editora. Antes de se tornar Perito Criminal Federal, atuou como desenvolvedor de sistemas Web e professor universitário em Computação.