Investigação de Crimes Cibernéticos

A carreira da Computação Forense

Deivison Pinheiro Franco, deivison.franco@bancoamazonia.com.br, Banco da Amazônia

A procura por formação na computação forense ainda é novidade e abre frentes para o profissional no Brasil. Abolir completamente a prática de crimes é impossível, mas é possível minimizar suas ocorrências através de sua investigação, permitindo que novas técnicas para o combate aos crimes digitais sejam descobertas e que criminosos cibernéticos não fiquem impunes. E é aí que os peritos forenses computacionais atuam – com o intuito de determinar e provar dinâmica, autoria e materialidade de ilícitos computacionais.

Estamos na era digital onde o computador, a Internet e muitos outros recursos tecnológicos fazem parte, cada vez mais, do nosso cotidiano, trazendo consigo inúmeros benefícios a todos. Entretanto, com o advento de tantas vantagens vem também a possibilidade da realização de novas práticas ilícitas e criminosas, junto ao avanço tecnológico e a partir da computação ubíqua ("onipresença" da informática no cotidiano das pessoas).

Cada vez mais estamos conectados com o mundo, todos com todos, através de celulares, tablets, computadores etc., e esses equipamentos já possibilitam a realização de quase tudo em questão de poucos minutos e sem sair de casa – desde a conhecer pessoas, como fazer compras – tudo isso a poucos cliques de "distância" [1].

Todo esse aparato tecnológico facilita, e muito, a vida de todos, mas inevitavelmente acaba por se tornar um novo meio para a prática de delitos. Tal fato decorre da facilidade do anonimato quando se está na frente de um computador aliada a técnicas para omitir quaisquer evidências que comprovem um crime e seu autor, já que em uma investigação sabe-se o IP do computador, mas não quem é o criminoso digital.

Crimes Cibernéticos

Para a Symantec, tal como a criminalidade tradicional, a cibercriminalidade pode assumir muitas formas e pode ocorrer quase a qualquer hora ou lugar. Os criminosos cibernéticos usam métodos diferentes segundo suas habilidades e seus objetivos. Esse fato não deveria ser surpreendente, afinal, o crime cibernético é nada mais que um "crime" com um ingrediente "informático" ou "cibernético" [7].

Ainda para a Symantec, com base nos diferentes tipos de crime cibernético, o define de forma precisa como qualquer delito em que tenha sido utilizado um computador, uma rede ou um dispositivo de hardware. O computador ou dispositivo pode ser o agente, o facilitador ou a vítima do crime. O delito pode ocorrer apenas no computador, bem como em outras localizações. Para compreender melhor a ampla variedade de crimes cibernéticos é preciso dividi-los em duas categorias gerais, definidos para os efeitos desta pesquisa como crimes cibernéticos do tipo I e II. No primeiro tipo o computador é apenas uma ferramenta de auxílio aos criminosos na prática de crimes conhecidos, como sonegação fiscal, compra de votos em eleições, tráfico de entorpecentes e falsificação de documentos e outros, ou seja, se o dispositivo não existisse, tal crime seria praticado da mesma forma. Já no segundo, o computador é a peça central para a ocorrência do crime, ou seja, se o dispositivo não existisse, tal crime não seria praticado [7].

Invasão de computadores, criação de comunidades virtuais para fazer apologia ao uso de drogas, envio de vírus de computador por e-mail, além do impulso que dá a crimes antigos como pornografia infantil, estelionato, engenharia social, entre outros [1]. Como é possível observar a partir dessas definições, o cibercrime pode englobar uma gama muito ampla de ataques, e compreender essa variedade de crimes cibernéticos é importante visto que seus diferentes tipos requerem atitudes diferentes para melhorar a segurança computacional, haja vista que a eliminação de fronteiras oferecida pela Internet acaba gerando sérias dificuldades para o combate a esses tipos de crimes, facilitando sua prática e ocorrência onde vítima e criminoso podem encontrar-se em países distintos [4].

Com essa nova modalidade de crimes e os mais diversos danos que podem causar, surge a necessidade de profissionais especializados, com amplo conhecimento em computação, segurança da informação, direito digital e outras áreas afins, com capacidade suficiente para investigar quem, como e quando um crime cibernético foi praticado, ou seja, um profissional capaz de identificar autoria, materialidade e dinâmica de um crime digital, já que em um local de crime convencional, um vestígio pode significar desde um instrumento deixado no ambiente pelo criminoso, a um fio de cabelo do mesmo. Entretanto, na informática os vestígios são digitais – zeros e uns, dados lógicos que compõem a evidência digital, a qual poderá ser desde conversas em chats, histórico de internet, programas etc., a arquivos excluídos intencionalmente pelo criminoso [4].

Investigação de Crimes Cibernéticos e a Atuação do Perito Forense Computacional

Segundo o dicionário Aurélio de Língua Portuguesa, o termo forense significa "que se refere a foro judicial". Já a perícia, de acordo com o mesmo dicionário, é a prática que um profissional qualificado exerce, neste caso denominado de perito. Vistoria ou exame de caráter técnico e especializado. Dessa forma, as ciências forenses são desenvolvidas 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.

A forense computacional, ou computação forense, visa os mesmos eventos relatados acima, só que na área tecnológica, buscando pistas virtuais que possam descrever o autor de ações ilícitas, a fim de suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. Sendo assim, ela é a ciência responsável por coletar provas em meios eletrônicos que sejam aceitas em juízo, tendo como principal objetivo a aquisição, a identificação, a extração e análise de dados que estejam em formato eletrônico e/ou armazenados em algum tipo de mídia computacional [8].

Ante ao exposto, a perícia forense computacional tem como objetivo principal determinar a dinâmica, a materialidade e a autoria de ilícitos ligados à área de informática, tendo como questão principal a identificação e o processamento de evidências digitais em provas materiais de crime, por meio de métodos técnico-científicos, conferindo-lhe validade probatória em juízo. Para isso, o perito forense computacional averigua e investiga os fatos de uma ocorrência digital e propõe um laudo técnico para entendimento geral de um episódio, comprovado através de provas, juntando 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 equipamentos computacionais e eletrônicos. De tal forma que um laudo ou um relatório técnico imparcial seja gerado para que fiquem claras as comprovações dos fatos fundamentados, a fim de se nortear os julgadores do acontecido. Sendo que, no campo da informática, os principais exames forenses realizados estão entre exames periciais em dispositivos de armazenamento computacional como HDs, CDs, DVDs, Blu-Rays, pendrives etc. e outros dispositivos de armazenamento como smartphones, smart tvs, tablets, sites, vídeo games, e-mails [4]. Cabendo ressaltar que em alguns casos é necessária a realização de procedimentos ainda no local do delito, para que possíveis evidências não sejam perdidas, pois no caso de um flagrante é possível encontrar o computador do criminoso ligado, quando necessário proceder a análise no local [8].

A importância do papel do especialista em computação forense, ou perito forense computacional, vem ganhando grande relevância e destaque devido ao crescimento dos crimes cibernéticos. A partir dessa situação surge a necessidade de profissionais capazes de elaborar laudos a fim de se determinar a dinâmica, a materialidade e a autoria de ilícitos eletrônicos, para que se viabilize e possibilite aplicação de punição para determinado caso que envolva esses tipos de crimes [6].

Atualmente a computação forense já faz parte da rotina policial, pois não é mais novidade alguma, em um local de crime, encontrar-se um ou mais computadores, os quais necessitem de um profissional apto a investigar e periciar o equipamento em questão, o qual pode se tornar, dependendo da informação encontrada, a peça chave para a comprovação de um crime.

A Carreira do Perito Forense Computacional

Reconstruir o passado, constatar a materialidade e apurar a autoria de incidentes cometidos com o requinte dos bits. Esta é a função da perícia digital ou forense digital, carreira que mescla a formação jurídica com a tecnologia da informação e que é crescente na esfera pública e privada, à medida em que conflitos, fraudes, furtos e agressões passam a ser cometidas por intermédio de dispositivos informáticos e telemáticos, de um computador de mesa a um dispositivo móvel celular [5].

A forense computacional é uma das áreas da computação em fase de ascensão e já é possível encontrar especialização em abundância nessa área no país, uma vez que está sendo bem difundida ultimamente em relação a alguns anos atrás, devido à crescente prática de atividades ilícitas através da tecnologia digital [4]. Dessa forma, com as mudanças no paradigma tecnológico atual, surge aos poucos a necessidade cada vez maior de um profissional com conhecimento em perícia forense computacional (ou digital), capazes de investigar e produzir laudos periciais que provem autoria e materialidade de um delito eletrônico [6].

O estudo e a procura por formação profissional na computação forense ainda é novidade para muitos e está desenvolvendo-se principalmente pela necessidade do combate aos crimes eletrônicos. Os profissionais na área podem ser chamados nos mais diversos lugares que precise de algum serviço minucioso o qual envolva equipamentos informáticos e têm regras a seguir e providências definidas a tomar, tanto para obter credibilidade no que fazem, quanto para que seu trabalho não tenha sido em vão e desconsiderado em uma audiência judicial, onde um parecer técnico ou laudo será necessário.

Os profissionais que atuam na área de forense computacional são indivíduos geralmente chamados de peritos por terem um grande nível de conhecimento em computação e por investigarem os crimes de natureza tecnológica. Nesse contexto, esses profissionais devem reunir um conjunto de características conforme apresentado no Quadro 1.

- Conhecimento e entendimento profundo de segurança da informação, direito digital e sistemas computacionais, bem como das características de funcionamento de sistemas de arquivos, programas de computador e padrões de comunicação em redes de computadores;
- Familiaridade com as ferramentas, técnicas, estratégias e metodologia de ataques conhecidos, inclusive as que não se tem registo de ter ocorrido, mas que já são vistas como uma exploração em potencial de uma determinada vulnerabilidade de um sistema;
- Faro investigativo para perceber rastros sutis de ações maliciosas - Esmero pela perfeição e detalhes. Sempre deve haver rastros, mesmo que muito sutis;
- Entendimento sobre o encadeamento de causas e consequências em tudo o que ocorre num sistema para construir a história lógica formada por ações maliciosas ou normais que já tenham ocorrido, que estejam em curso e que possam vir a acontecer;
- Conhecimento da legislação envolvida;
- Conhecimento das diretivas internas das empresas e instituições envolvidas no processo investigativo, com especial atenção às limitações como diretivas de privacidade, sigilo e escopo ou jurisdição de atuação;
- Cuidado com a manipulação e preservação de provas legais em potencial, pois o que não é visto como prova hoje pode vir a ser uma prova e então é bom ter sido preservada o suficiente para ser aceita em um tribunal;
- Experiência ao examinar os rastros em um incidente perceber o nível de sofisticação e conhecimento de um atacante, especialmente interessante se o atacante usa subterfúgios para parecer menos capaz, como deixar rastros óbvios e parecer um ataque simples para ocultar ações maliciosas muito mais perigosas e muito mais escondidas.

Quadro 1 - Características dos profissionais da área

Mas por onde começar para se tornar um perito forense computacional?

Primeiramente, fazer um curso de graduação que envolva computação é imprescindível para se trabalhar na área. Em seguida optar por cursos de pós-graduação especifica e, como a evolução tecnológica é dinâmica, é importante estar sempre atualizado e fazer cursos e certificações da área.

Além disso, a formação do profissional aspirante a perito, que deve ser aprofundada em tecnologia e direito, deve demonstrar experiências em frameworks, compliance e melhores práticas previstas na tecnologia da informação como SOX, COBIT, ITIL, PCI, ISO 27001, além da legislação básica

brasileira, Código Civil, Código Penal, Consolidação das Leis do Trabalho, e principalmente, normas processuais e procedimentais que regulamentam a produção da prova pericial no Brasil.

A formação ideal deve ser a jurídica juntamente com a técnica, eis que mais do que saber agir tecnicamente ou conhecer a intimidade das falhas e dos sistemas, este profissional precisa atuar na linha tênue que separa uma perícia homologada, de uma produção probatória nula, ilícita ou ilegítima. Além do que, nesta profissão, saber escrever e dar significado a zeros e uns é fundamental [6].

O profissional pode atuar na área pública ou privada. Na área pública, deve peticionar em juízo sua habilitação que será ou não deferida pelo juiz, e em algumas comarcas, pode-se auxiliar o Ministério Público e Delegacias não especializadas também apresentando-se em petição escrita instruída de curriculum, antecedentes criminais e casos que atuou [5]. Pode-se igualmente ser um perito policial, integrante do Instituto de criminalística dos Estados ou da Polícia Federal (mediante concurso). Já na área privada, os profissionais podem atuar ou em forense corporativa integrando uma equipe multidisciplinar composta por profissionais da área jurídica e técnica, ou como assistente técnico, representando a parte na perícia, sendo, portanto, alguém de sua confiança [6].

A carreira de perito digital é hoje uma profissão em ascensão e há várias universidades no país que oferecem cursos de pós-graduação e até mestrado na área, como a Universidade Presbiteriana Mackenzie, a Universidade Potiguar e a Universidade de Brasília, por exemplo. O Quadro 2 apresenta algumas informações para se começar na caminhada da carreira profissional de perito forense computacional.

Cursos de Pós-graduação
- Universidade Presbiteriana Mackenzie
- Universidade Potiguar
- Universidade de Brasília

Certificações em Ferramentas
- EnCE (EnCase Certified Examiner)
- ACE (AccessData Certified Examiner)

Certificações em Cursos
- CCFT (Certified Computer Forensic Technical)
- CEH (Certified Ethical Hacker)
- CHFI (Certified Hacker Forensic Investigator)
- ACFEI (American College of Forensic Examiners Institute)
- DSFE (Data Security Forensics Examiner)

Empresas de Certificações e Treinamentos no Brasil
- Data Security - Segurança da Informação e Forense Computacional
- Clavis - Segurança da Informação e Forense Computacional
- Legaltech - Consultoria, Pericia e Treinamento
- TechBiz - Forense Digital
- 4Linux - Free Software Solutions

Eventos
- ICCYBER - Conferência Internacional em Crimes Cibernéticos
- ICOFCS - Conferência Internacional sobre Ciência da Computação Forense
- Congresso Crimes Eletrônicos e Formas de Proteção
- SBSeg - Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais
- H2HC - Hackers To Hackers Conference

Quadro 2 - Websites e outras dicas

Por fim, é interessante mencionar que os honorários das perícias de qualquer natureza, podem variar entre R$ 7.000,00 à R$ 100.000,00, mas a boa rentabilidade reflete grandes responsabilidades. Aos pretendentes à área, a profissão é rentável, mas exige muito, pois pode-se ter centenas de pericias positivas, mas basta um deslize ou uma evidência clara que não foi encontrada para que todo o histórico seja destruído. Cabe avisar que qualquer conduta impensada como um simples comando para listar o diretório de um sistema operacional, pode significar a perda de dados importantes e, até mesmo, milhares ou milhões para as partes envolvidas [5].

Considerações Finais

É indubitável que estamos cada vez mais dependentes da tecnologia e é natural que os criminosos usufruam das mesmas vantagens tecnológicas que nós.

Pessoas mal intencionadas utilizam esse recurso para ganhar dinheiro e até mesmo para cometer crimes na rede e abolir completamente a prática de crimes é impossível, mas é possível minimizar suas ocorrências através de sua investigação, não permitindo que novas técnicas para o combate aos crimes digitais sejam descobertas e que criminosos cibernéticos fiquem impunes e é ai que os peritos forenses computacionais atuam – com o intuito de determinar e provar dinâmica, autoria e materialidade de ilícitos computacionais, como os CSI do século XXI.

Recursos

[1] CARDOSO, Nágila Magalhães. **A Importância dos Profissionais em Computação Forense no Combate aos Crimes Tecnológicos**. Revista Espírito Livre, n.32, p.58-60. 2011.

[2] CASEY, Eoghan. **Handbook of Computer Crime Investigation Forensics - Tools and Technology**. 2ª Edição. California: Academic Press, 2003.

[3] ELEUTÉRIO, Pedro. M. S; MACHADO, Márcio. P.. **Desvendando a Computação Forense**. 1ª Edição. Novatec, 2010.

[4] FRANCO, Deivison Pinheiro. **CSI do Século XXI**. Revista Convergência Digital, n.2, v.2, p.24-26. Universo Online, 2012.

[5] MELO, Gilberto. **A Profissão do Futuro: Como Ser Um Perito Digital**. 2012. http://gilbertomelo.com.br/jurisprudencias-e-noticias/90/2865-a-profissao-do-futuro-como-ser-um-perito-digital.

[6] MILAGRE, José Antonio. **Empregos, Certificação e Licença Para Ser Perito Digital**. http://josemilagre.com.br/blog/2011/01/25/empregos-certificacao-e-licenca-para-ser-perito-digital.

[7] SYMANTEC. **O Que é Crime Cibernético?** 2012. http://br.norton.com/cybercrime/definition.jsp

[8] TOLENTINO, Luciano Cordova; SILVA, Wanessa da; e MELLO, Paulo Augusto M.S. **Perícia Forense Computacional**. Revista Tecnologias em Projeção, n.2, v.2, p.26-31. 2011.

Sobre o Autor

Deivison Pinheiro Franco é Técnico Científico em TI, Analista Pleno em Arquitetura de Infraestrutura Computacional do Banco da Amazônia. Mestrando em Computação Aplicada pelo Programa de Pós-Graduação em Engenharia Elétrica – PPGEE da Universidade Federal do Pará – UFPA, possui especialização em Ciências Forenses com Ênfase em Computação Forense pelo Centro Universitário do Estado do Pará – CESUPA, em Suporte a Redes de Computadores e Tecnologias Internet pela UFPA e graduação em Processamento de Dados pela Universidade da Amazônia – Unama. É professor nos cursos superiores de Análise e Desenvolvimento de Sistemas e de Redes de Computadores da Faculdade de Castanhal – FCAT e no curso de Especialização em Ciências Forenses do CESUPA. É Colunista das Revistas Convergência Digital e Segurança Digital. Além de atuar como Perito Forense Computacional, também é Auditor de TI e Pentester.