88 – Junho 2007

Primeiro contato com a Ciência Forense

Novas profissões e nichos de mercado surgem em função de novas necessidades, enquanto outras profissões simplesmente se renovam. Isso vem ocorrendo com os profissionais de perícia técnica, o que têm despertado enorme interesse dos jovens estudantes e também dos experientes profissionais de tecnologia da informação. Entretanto, antes de falar mais diretamente sobre Prática Forense é preciso entender o conceito e o contexto em que o termo se aplica.

Ciência Forense é uma área interdisciplinar que aplica um amplo espectro de ciências com o objetivo de dar suporte - respondendo perguntas - às investigações relativas ao sistema legal, mais precisamente ligadas à justiça civil e criminal. Entre seus desafios está a identificação do crime, o rastreamento das etapas que o precederam, a localização e preservação de evidências e a geração de documento de suporte legal.

Dentro do contexto eletrônico, também chamada de Forense Digital ou *Computer Forensics*, podemos descrevê-la como a ciência que realiza inspeções sistemáticas em sistemas de computador e suas informações para evidenciar ou suportar a evidência de crime. Forense Digital requer conhecimento especializado passando pela simples coleta de dados e a preservação de provas. Estamos necessariamente falando de ambientes eletrônicos, redes de computadores, sistemas operacionais e aplicações que exigem do perito, além de conhecimento especializado, ferramentas que o auxiliem nas diferentes etapas da investigação, assim como o que ocorre com a perícia criminal tradicional, que lança mão de luvas, lupas, microscópios e demais aparatos para identificar trajetórias, digitais e outros elementos de investigação.

Alguns dos cenários comuns onde se aplica a prática forense digital:

- Abuso de Internet por funcionários
- Acesso não autorizado a dados e informações sigilosas
- Dano a ativos
- Espionagem industrial
- Crime de fraude
- Roubo de identidade
- Investigação de Pedofilia

Em geral os trabalhos se iniciam com a identificação de acessos não autorizados, atividades proibidas ou reguladas, uso ilegal de sistemas e informações, e para isso, realizam inspeções em discos rígidos, mídias removíveis, bancos de dados e qualquer outra potencial fonte de informação pericial.

Podemos dividir as etapas da Forense Digital da seguinte forma:

- Identificação de fontes de informação e evidência/prova
- Preservação da evidência/prova
- Análise da evidência/prova

- Documentação de atividades de descobertas e conclusões

O exercício desta prática precisa encontrar o equilíbrio entre a abordagem puramente técnica e a abordagem puramente legal, pois precisa estar aderente aos padrões de evidência reconhecidos pela lei usando a técnica como instrumento.

Muitas são as ferramentas utilizadas na prática forense digital, onde se destacam as seguintes categorias:

- Duplicadores de mídia
- Coletores de log
- Identificadores de configuração
- Rastreadores de dados e strings
- Copiadores de memória
- Duplicadores de sistema operacional
- Mapeadores de rota de conexão
- Extratores de inventário
- Recuperadores de dados
- Decriptadores ou decifradores de código
- Analisadores de esteganografia
- Testadores de sistema

O famoso detetive Sherlock Holmes que nos perdoe, pois diante da criatividade dos criminosos e da necessidade de tantos aparatos, já não se consegue fazer praticamente nada com a velha dupla: cachimbo e lupa.

Este tema tem consumido ultimamente boa parte das minhas horas de estudo e pesquisa, mais precisamente focadas nos campos de fraude eletrônica e contra-espionagem. É, sem dúvida, um nicho de grande potencial profissional, motivado pelo fértil momento em que os setores público e privado discutem os riscos da informação de forma integrada, colocando os aspectos legais e técnicos em igual condição de importância.

Marcos Sêmola é Diretor de Operações de Information Risk da Atos Origin em Londres, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. Professor da FGV com especialização em Negociação e Estratégia pela London School, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br