Perícia e Investigação Forense Computacional: Maturidade?

O crescente número de crimes e fraudes praticadas com o requinte dos bits fez surgir uma necessidade corporativa e governamental de peritos e especialistas em investigar e reconstituir fatos praticados por intermédio de Computadores. Falamos da Computação Forense ou Computer Forensics, hoje se estendendo aos dispositivos móveis, a chamada Mobile Forensics.

Para atuar na área tem-se apreciado formação tecnológica e jurídica, ainda que uma das duas seja de nível técnico ou especialização, bem como profundo conhecimento processual para se detectar e conhecer procedimentos sólidos, válidos, lícitos e éticos. Tal ponto vem nos preocupando recentemente. Ser perito é atuar como "olho" da corporação ou do magistrado, é ser imparcial e não se contentar com exames superficiais ou "sob o capô" do "veículo". Um perito jamais trabalha na camada de abstração criada pelo sistema de arquivos aos usuários, até porque presume-se que este seja algo além de mero usuário. Estamos lidando com a vida de empresas e pessoas, e não se pode tolerar exames abstratos e sem o atendimento a procedimentos de consenso mundial.

A medida em que não nos contentamos com a camada de abstração criada por sistemas e aprofundamo-nos na pesquisa computacional, encontramos informações mais precisas, e que a princípio no "capô", não mais existiam, como por exemplo, arquivos excluídos, ocultos, esteganografia, etc. Citamos o caso onde recebemos equipamentos para análise de eventual disco virtual criptografado. Evidentemente, o disco estava lá, pois haviam arquivos de montagem na máquina, porém isso por si só não era suficiente para concluir em processo indutivo que

existiam informações ocultadas no disco. Tínhamos um outro desafio, qual seja, quebrar a criptografia de 1024 bits. Antes que iniciássemos um ripper decidimos analisar de maneira forense um retrato da memória e dos arquivos de hibernação, buscando por queryes normalmente lançadas por programas tipo bestcript e truecript. Após a verificação constatamos, a senha estava lá, límpida, fossilizada na memória. Ou seja, em uma análise "sob o capô" poderíamos muito bem dizer à empresa: "Não encontramos nada". E teríamos mais um criminoso ou fraudador não penalizado pela inércia de um profissional de computação forense.

Outra premissa que deve ser enfrentada é que não precisamos de super-heróis. Se não podemos descobrir a senha cifrada, capturemos ela quando estava a caminho da cifragem. Conhecemos casos em que o perito utilizou-se de trojans forenses para infectar o investigado. Não fica difícil concluir que a prova foi desconsiderada no processo judicial de concorrência desleal. Não precisamos recuperar completamente o passado, mas é preciso que se tenha ciência de que uma recuperação parcial pode ser suficiente para retratar o que realmente ocorreu, com ética e alta carga valorativa para um eventual processo judicial, a critério da direção.

Ética é outra premissa fundamental. Imagine que você é procurado por um alto-executivo de uma empresa que de alguma maneira teve fotos em situação sexual divulgadas na rede. Ele chega no laboratório e diz a você que paga o quanto for para que seja realizada uma alteração nas imagens buscando comprovar uma "montagem". Tecnicamente contamos com procedures de edição de Exifs (negativo das imagens digitais) e Timestomp que prontamente podem "transformar um original em montagem" de maneira indetectável. Porém tal postura é imatura e demonstra um abuso de técnicas que ao aprendidas, deveriam ser utilizadas para a finalidade nobre que é investigação dos crescentes crimes eletrônicos.

A Perícia Digital literalmente tem o poder em mãos, podendo

criar ou desfazer provas digitais. Porém sabe-se que a finalidade da ciência é axiliar empresas e judiciário na apuração de materialidade e autoria de delitos eletrônicos. Maturidade neste aspecto é ter consciência de que nada é impossível em tecnologia da informação, mas, principalmente, é saber que ser ético é tão ou mais importante do que ser um bom profissional.

Siga no Twitter: http://www.twitter.com/periciadigital