



CENTRO UNIVERSITÁRIO DA GRANDE DOURADOS

ROBSON TIROTTI FELIPE

PERÍCIAS EM MEIOS ELETRÔNICOS: MAXIMIZANDO O
VALOR DA PROVA

Dourados/MS

2008



CENTRO UNIVERSITÁRIO DA GRANDE DOURADOS

ROBSON TIROTTI FELIPE

PERÍCIAS EM MEIOS ELETRÔNICOS: MAXIMIZANDO O
VALOR DA PROVA

Artigo apresentado ao Departamento de Pós-Graduação do Centro Universitário da Grande Dourados – UNIGRAN, em Dourados/MS, como Trabalho de Conclusão de Curso para obtenção do Título de Especialista, no Curso de Pós-Graduação *Lato Sensu* em Direito Eletrônico e Tecnologia da Informação, sob a orientação do Professor Especialista José Antonio Maurilio Milagre.

Dourados/MS

2008

PERÍCIAS EM MEIOS ELETRÔNICOS: MAXIMIZANDO O VALOR DA PROVA

Robson Tirotti Felipe¹

RESUMO: O presente artigo trata das peculiaridades do exame pericial realizado em meios eletrônicos, o que exige a atuação de profissional devidamente especializado. O perito deve adotar metodologia específica, visando a otimizar a pesquisa, coleta, manuseio, preservação, transporte e análise dos vestígios ditos virtuais. A preocupação com tal metodologia ainda é pequena, mas já existem padrões internacionais definidos sendo aplicados experimentalmente (OLIVEIRA, GUIMARÃES, GEUS, 2002). A finalidade precípua destas linhas é demonstrar a importância da adoção dos procedimentos padronizados adequados, com ênfase na preservação, o que acarreta uma maior valoração da prova eletrônica diante do sistema processual que vigora em nossos Tribunais.

Palavras-chave: Perícias em Informática, Computação Forense, Perito, Valor da Prova.

ABSTRACT: This article treats the computer forensics peculiarities, which require appropriate personnel performance. The forensic expert may adopt a specific methodology to improve the searching, seizing, handling, maintaining, packaging and examination of digital evidence. The concern about it is modest, but there are already international standards applied experimentally (OLIVEIRA, GUIMARÃES, GEUS, 2002). The main purpose of this article is to demonstrate the importance of correct and standardized procedures, focusing evidence maintaining, what lead digital evidence greater value to Brazilian Tribunal's trials.

Keywords: Computer Analysis, Computer Forensics, Expert, Proof Value.

1 INTRODUÇÃO

A palavra perícia deriva do latim *peritia* e significa habilidade especial. É uma modalidade de prova que se constitui em exame procedido por pessoa (perito) que tenha determinados conhecimentos técnicos, científicos, artísticos ou práticos acerca de um fato, circunstâncias ou ainda condições pessoais a ele inerentes (MAGNO, 2005). Segundo Zarzuela (1995), a perícia implica a apreciação, interpretação e descrição dos fatos ou circunstâncias. Tais conhecimentos técnico-científicos integram uma disciplina conhecida como Criminalística, cujas áreas de atuação estão relacionadas ao próprio desenvolvimento da Ciência, pois suas novas descobertas também passam a auxiliar a Justiça com a produção da

¹ Perito Criminal do Instituto de Criminalística de São Paulo, pós-graduando em Direito Eletrônico e Tecnologia da Informação pelo Centro Universitário da Grande Dourados – UNIGRAN.

prova técnica. Existem, portanto, diversos tipos de perícia não discriminados diretamente no Código de Processo Penal (CPP)²; outras advêm de legislação específica³; mas há ainda outras que independem de qualquer previsão legal (ESPINDULA, 2006) como, por exemplo, a fonética, a contabilidade, a modelagem e a computação forense.

Esta última nos chama a atenção nem tanto por seu caráter recente, mas pelo avanço e popularização da Internet, que traduziu uma nova realidade, extremamente dinâmica: *chats, blogs, fotologs, Orkut, MSN, webcams, homebanking, e-mail, e-commerce e second life* passaram a fazer parte do cotidiano de um indivíduo num piscar de olhos, ou melhor, num clique de *mouse*. Nas palavras de Resina (2006, p.27), a Internet “tornou-se, além de meio de comunicação e entretenimento, ferramenta indispensável de trabalho na vida de todos”, o que se constitui um panorama favorável não só para investidores, mas também para indivíduos desonestos, com intenções escusas que, com a prática de crimes, acabam por lesar cidadãos, organizações e instituições (COSTA, 2003). Esses “atos e fatos ocorridos em virtude, ou através da Internet exigem atuação enérgica do Direito, que não deve estar ausente desta nova realidade” (RESINA, 2006, p.28).

Concebe-se a computação forense como o ramo da Criminalística voltado, segundo Costa (2003), para o estudo e avaliação de situações que envolvam a computação como meio para se cometer ilícitos, o que “envolve a preservação, identificação, análise e estruturação de evidências armazenadas em computadores [...]” (SCUDERE, 2006, p.210).

Entretanto, bem ressalta Milagre (2008) que a computação forense apresenta peculiaridades que a diferem das outras frentes da Criminalística: as evidências são “virtuais”, ou seja, na maioria das vezes têm-se dados e informações e não um objeto físico palpável; muitos desses dados são extremamente voláteis, ou seja, são facilmente perdidos; os métodos de exame não são únicos e não há padronização nas técnicas de coleta, que devem ser selecionadas pelo perito caso a caso face à variedade de sistemas, programas e ações ilícitas.

Destarte, a conduta do perito deve ser a mais cautelosa possível, de modo a assegurar a integridade e autenticidade das evidências, maximizando o valor da prova obtida em meios eletrônicos, já que procedimentos inadequados podem jogar por terra o que seria, talvez, a única possibilidade de se ter a materialidade ou autoria do delito.

² São modalidades de perícia previstas no CPP: reprodução simulada dos fatos, perinecrocópica, documentoscópica, de laboratório, em local de crime contra o patrimônio, em local de incêndio, em instrumentos de crime, necrocópica, exumação, vistoria de busca e apreensão, psiquiátrica de averiguação de insanidade mental do acusado.

³ Como exemplo, há os exames em entorpecentes, previstos na Lei 11.343/06 (Lei dos Tóxicos) e os exames em locais de crimes contra o meio ambiente, previstos na Lei 9.605/98.

A finalidade destas linhas é, portanto, realizar uma revisão bibliográfica sobre como os procedimentos e metodologias para as perícias realizadas em meios eletrônicos são tratados atualmente, elencando e analisando os principais itens referentes à coleta, preservação e análise adequada dos respectivos vestígios.

2 PROCEDIMENTOS EM PERÍCIAS DE LOCAIS E INSTRUMENTOS DE CRIMES ELETRÔNICOS

2.1 ASPECTOS PRELIMINARES

A elaboração de qualquer laudo pericial, especialmente aquele proveniente da análise de evidências digitais, está diretamente ligada às requisições de exames periciais ou mandados judiciais recebidos, pois são o meio pelo qual a autoridade policial ou judiciária determina a realização de trabalhos técnico-científicos necessários à perfeita configuração da infração penal. Tais documentos devem mencionar de forma compreensível o objeto da perícia, o objetivo do exame, bem como todas as informações conhecidas sobre o caso, formulando-se, sempre que possível, quesitos específicos (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2000). Tocchetto (2005) vai além e afirma que tais quesitos devem ser formulados de forma clara, objetiva e precisa. É por meio desses documentos que o perito criminal direcionará o seu trabalho, já que se torna inviável a realização de exame pericial em meio eletrônicos sem referidas informações.

Porém, o aspecto mais importante, quando se fala em valoração da prova pericial, é lembrado por Milagre (2008): a Constituição Federal veda a obtenção de provas obtidas por meios ilícitos ou ilegítimos. Isto permite inferir que o perito deve estar adstrito ao mandado, respeitando seus limites e restrições, atentando-se para o objeto do mesmo, jamais o extrapolando, vindo a analisar outros dados que não os de interesse. Tal conduta certamente será motivo de anulação do trabalho pericial, além de ser falta de ética e crime tipificado pela Lei 9296/96, apenado com reclusão⁴. Por conseguinte, o perito deve possuir conhecimentos sobre as limitações legais vigentes no país de modo que as provas obtidas sejam válidas perante a lei (TREVENZOLI, 2006).

⁴ Art.10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
Pena: reclusão, de dois a quatro anos, e multa.

Certamente, os limites estabelecidos não implicam que o perito deve ignorar vestígios de conduta ilícita (distinta do escopo da perícia) ou fatos e atos de presumível interesse policial ou jurídico, descobertos acidentalmente (obviamente respeitando os limites e restrições) quando da análise do objeto, sob pena de ser negligente e conivente. O procedimento correto a ser adotado é consignado por Milagre (2008, p.27, tradução nossa) ao trazer a postura taxativa do Departamento de Justiça Norte-Americano: “Informação incriminadora fora do escopo da busca: Pare! Notifique as pessoas apropriadas e aguarde instruções⁵”. Tal conduta traduz o padrão de moral e ética esperados, já que, assim, o perito nem extrapola os limites do mandado judicial nem é conivente com o encontrado.

Quando a autoridade requisitar o exame, deverá fazê-lo ao diretor da repartição em que o perito criminal está lotado, nos termos do artigo 178 do CPP⁶. Cabe, portanto, ao diretor do Instituto de Criminalística a designação do profissional que irá executar a perícia, que saberá qual melhor desempenhará a tarefa, observando-se a questão da especialização profissional necessária para cada caso (DOREA; STUMVOLL; QUINTELA, 2006).

Exames feitos por profissionais sem formação específica na área computacional podem dar margem a questionamentos das partes e influir no convencimento do magistrado. Além disso, menos familiarizados com as peculiaridades da perícia informática, podem, inadvertidamente, alterar vestígios importantes ou deixar de observar itens que forneceria informações preciosas sobre o ilícito. Vale lembrar ainda que, em uma análise forense, o perito busca as evidências de um crime, deixadas por “programador que não tem o interesse de ser descoberto” (FARMER e VENEMA, 2000 *apud* OLIVEIRA; GUIMARÃES; GEUS, 2002), o que por si só já dificulta o exame e exige pessoal capacitado.

2.2 ASPECTOS LEGAIS DA PRESERVAÇÃO

É indiscutível a importância do exame de corpo de delito em uma infração penal, que se configura obrigatório quando aquela deixa vestígios. Ora, delitos informáticos deixam muitos vestígios (MILAGRE, 2008). Tamanha é sua relevância, que nem a própria confissão do acusado pode supri-lo, nos termos do artigo 158 do CPP⁷. Além disso, a inexistência do

⁵ “Incriminating information outside scope of the warrant: Stop! Notify appropriate personnel, wait for instruction”.

⁶ Art. 178. [...], o exame será requerido pela autoridade ao diretor da repartição, juntando-se ao processo o laudo assinado pelos peritos.

⁷ Art. 158. Quando a infração penal deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado.

exame nas infrações que deixem vestígios é causa de nulidade da ação penal (artigo 564, III, b, do CPP⁸), ressalvado o caso de desaparecimento deles, hipótese em que se admite a prova testemunhal (artigo 167⁹ do CPP). Obviamente, o desaparecimento dos vestígios não pode ser resultante da inércia ou inaptidão dos órgãos estatais incumbidos da persecução penal (REIS e GONÇALVES, 2005). Interessante notar que nos crimes cometidos contra a propriedade imaterial, a falta do exame pericial, quando houver vestígios, acarretará o não-recebimento da denúncia ou da queixa pelo magistrado (artigo 525¹⁰ do CPP). Ressalte-se que aí está incluído o crime de violação de direito autoral que, na maioria das vezes, enseja exame em computadores, mídias e periféricos.

Um dos meios mais eficazes de o perito emitir seu juízo valor é pela pesquisa científica e análise acurada dos elementos de ordem material de um local de crime, necessariamente preservados (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2000).

O isolamento e a conseqüente preservação do local de infração penal é uma garantia de que o perito encontrará a cena tal como deixada pelos infratores e vítimas e, com isso, terá condições técnicas de analisar todos os vestígios. É também uma garantia para a investigação como um todo, pois haverá muito mais elementos a se analisar e carrear para o Inquérito Policial (ESPINDULA, 2006). Isso porque não apenas o computador é importante para a análise do perito computacional mas, dependendo do delito, também todas as condições e vestígios encontrados no próprio local.

A importância e a necessidade de se preservar e resguardar as informações de um local de crime, apesar de tardiamente, foi percebida pelos legisladores e, com a edição da Lei n.º 8.862/94, deu-se nova redação ao *caput* e incisos I e II do artigo 6.^º¹¹ do CPP.

Com a nova lei, a autoridade fica obrigada a comparecer ao local e efetuar a preservação até a chegada dos peritos criminais. Além disso, os objetos relacionados ao fato como, por exemplo, computadores e mídias, só poderão ser apreendidos após os exames efetuados pelos peritos, e se liberados por eles.

⁸ Art. 564. A nulidade ocorrerá nos seguintes casos: [...] III – por falta das fórmulas ou dos termos seguintes: [...] b) o exame do corpo de delito nos crimes que deixam vestígios, ressalvado o disposto no art. 167.

⁹ Art. 167. Não sendo possível o exame de corpo de delito por haverem desaparecido os vestígios, a prova testemunhal poderá suprir-lhe a falta

¹⁰ Art. 525. No caso de haver o crime deixado vestígio, a queixa ou a denúncia não será recebida se não for instruída com o exame pericial dos objetos que constituam o corpo de delito.

¹¹ Art. 6.º. Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

I – dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, **até a chegada dos peritos criminais** (grifo nosso);

II – apreender os objetos que tiverem relação com o fato, **após liberados pelos peritos criminais** (grifo nosso);

[...]

O *caput* do artigo 169 do CPP ressalta que a primeira providência da autoridade no local dos fatos é a preservação¹² e seu parágrafo único constitui uma garantia ao trabalho do perito. Se o local não estiver preservado e seu trabalho restar prejudicado, este fato deverá constar do laudo pericial, diante do que não se poderá argüir um trabalho mal-feito, inconclusivo, suspeito ou, até mesmo, falso. Devem ser discutidas quais as conseqüências das alterações, o que é extremamente difícil, pois serão feitas análises a partir de vestígios adulterados, acrescentados ou retirados. Na prática, muitos locais de crime, ainda quando não isolados ou preservados em nada prejudicam o trabalho da perícia (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2002). Segundo Espindula (2006), o perito não deve deixar de realizar o exame solicitado. Deve examinar tudo na forma em que encontrou e ter o cuidado de registrar tudo em seu laudo. Cumpre, ainda, ressaltar que o fato constitui crime se as alterações tiverem como dolo induzir o perito a erro, de acordo com artigo 347 e parágrafo único do Código Penal¹³.

A Secretaria de Segurança Pública do Estado de São Paulo editou, em 1999, a resolução 382/99, que dispõe sobre diretrizes a serem seguidas no atendimento de locais de crime, considerando que o rápido e correto atendimento de locais de crime contribui, sobremaneira, para o sucesso da investigação criminal, agilizando a liberação de pessoas e coisas. Considera, ainda, que o conhecimento de conceitos sobre local de crime facilita o entendimento das normas relativas à sua preservação bem como que da eficiente preservação do local de crime depende o bom resultado dos exames periciais, a fim de serem evitadas irreparáveis dificuldades à consecução do exame pericial e da investigação criminal (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2000).

Para o atendimento a um local de crime relacionado a meios eletrônico será de bom senso a presença de um perito computacional, quer seja nos casos em que o computador esteja *online*, quer seja nos casos em que o computador esteja desligado e o procedimento seja apenas de busca e apreensão. Não há dúvidas de que esse atendimento pericial deve ser

¹² Art. 169. Para o efeito de exame do local onde houver sido praticada a infração, a autoridade providenciará imediatamente para que não se altere o estado das coisas até a chegada dos peritos, que poderão instruir seus laudos com fotografias, desenhos ou esquemas elucidativos

Parágrafo único. Os peritos registrarão, no laudo, as alterações do estado das coisas e discutirão, no relatório, as conseqüências dessas alterações na dinâmica dos fatos.

¹³ Art. 347. Inovar, artificialmente, na pendência de processo civil ou administrativo, o estado de lugar, de coisa ou de pessoa, com o fim de induzir a erro o juiz ou o perito:

Pena – detenção de 3 (três) meses a 2 (dois) anos, e multa.

Parágrafo único. Se a inovação se destina a produzir efeito em processo penal, ainda que não iniciado, as penas aplicam-se em dobro.

extremamente rápido e que toda a polícia é responsável por esse atendimento^{14,15}. (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2000).

Já em seus artigos 1.^{o16} e 4.^{o17}, o texto da resolução ressalta a necessidade da preservação do local por parte do primeiro policial que atender à ocorrência, não abandonando o posto enquanto esta perdurar, sob pena de responsabilidade prescrita no artigo 5.^o, que elenca ainda vários aspectos de como se preservar adequadamente um local¹⁸ (POLÍCIA CIVIL DO ESTADO DE SÃO PAULO, 2000). Destaca-se a alínea “j” do inciso II de referido artigo, onde se consigna que os aparelhos (incluindo computadores) não devem ser ligados nem desligados. Tal tarefa caberá ao perito computacional.

2.3 REGISTRO, COLETA E TRANSPORTE

Embora detenha a chamada “fé pública”, a primeira providência do perito quando chegar ao local do crime deve ser o registro fotográfico e esquemático de toda a cena. Trata-se não somente de uma garantia ao trabalho do perito, mas também do início da cadeia de custódia, visando-se à integridade e autenticidade de todo o examinado. Milagre (2008, p.13) assevera que a concepção e adoção desse procedimento, “usado para manter e documentar a história cronológica da evidência” é fundamental em crimes nos quais se trabalha com “evidências absolutamente voláteis”.

¹⁴ Art. 24. A polícia como um todo e seus integrantes, individualmente, cada um dentro de sua parcela são responsáveis pelo rápido e correto atendimento de local de crime.

¹⁵ Art. 26. O rápido e correto atendimento do local de crime tem por objetivos contribuir para o sucesso da investigação criminal e minimizar a angústia das partes envolvidas.

¹⁶ Art. 1.^o O policial militar ao atender um local de crime deverá isolar e preservar adequadamente a área imediata e, se possível, a mediata, cuidando para que não ocorram, salvo os casos previstos em lei, modificações por sua própria iniciativa, impedindo o acesso de qualquer pessoa, mesmo familiares da vítima ou outros policiais que não façam parte da equipe especializada.

¹⁷ Art. 4.^o Enquanto perdurar a necessidade de que o local seja preservado, não poderá este ser abandonado em qualquer hipótese, devendo ficar guarnecido por pelo menos um policial. Efetivadas as medidas atinentes à preservação do local, dever-se-á providenciar o registro no respectivo distrito policial.

¹⁸ Art. 5.^o Deverão ser adotadas as seguintes normas, sob pena de responsabilidade:

[...]

II – preservar o local, não lhe alterando a forma em nenhuma hipótese, incluindo-se nisso:

- a) não mexer em absolutamente nada que componha a cena do crime, em especial não retirando, colocando ou modificando a posição do que quer que seja; [...]
- c) não recolher pertences; [...]
- f) não tocar nos objetos que estão sob sua guarda; [...]
- j) em locais internos, manter portas, janelas, mobiliário, eletrodomésticos, utensílios, tais como foram encontrados, não os abrindo ou fechando, **não os ligando ou desligando**, salvo o estritamente necessário para conter risco eventualmente existente (grifo nosso).

Depois dos primeiros registros da cena e de garantida a segurança do local e da equipe, o perito poderá voltar toda a sua atenção para a varredura minuciosa e sistemática da cena, ao final da qual deverá “ter a sensação de que nada ficou para trás, que nem um espaço deixou de ser examinado rigorosamente” (RODRIGUES, 2006, p.94).

Logicamente, a cena deve ser visualizada sob todos os aspectos forenses, e não apenas computacional. Portanto, “devem ser tomadas as precauções apropriadas a fim de minimizar qualquer chance de contaminação acidental de itens que possam ser posteriormente requisitados para outros exames laboratoriais como, por exemplo, impressões dígito-papilares e DNA¹⁹” (INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE, 2002, p.13, tradução nossa).

À medida que se procede à vistoria do local, deverão ser fotografados (ou filmados) todos os vestígios e peças de exame, nos pontos em que forem encontrados, tais como periféricos, gabinetes, mídias, documentos, inclusive monitores com as respectivas telas em exibição e cabos com as respectivas conexões. Segundo Trevenzoli (2006), no caso da tela em exibição, a fotografia será prova de algum programa aberto ou alguma operação em execução. Costa (2006) bem ressalta que deve ser dada especial atenção às mídias e aos discos rígidos removíveis. Os registros deverão vir acompanhados da descrição exata do que foi encontrado e de onde foi encontrado. “Também é útil registrar esse lugar em um esquema/croqui da cena ou da pessoa²⁰” (IOCE, 2002, p.14, tradução nossa). Rodrigues (2006) assevera que o levantamento fotográfico deve ser complementar, ou seja, juntas, as fotografias devem permitir uma visão global do ambiente.

Logicamente, depois de serem fotografados, os vestígios e as peças de exame precisam ser coletados a fim de serem transportados para o laboratório. Dando-se especial atenção à cadeia de custódia, a evidência (aqui compreendidos os vestígios e outras peças) deve ser devidamente embalada e lacrada, com a rotulação de cada pacote, onde deverá constar identificação, data e outros dados apropriados. Sampaio²¹ recomenda que, na medida do possível, o material arrecadado deverá estar acondicionado em embalagem original ou apropriada, de forma a evitar danos. Se for necessário acondicionar e transportar computadores, “deve-se colocar fita adesiva própria [ou lacres], de modo a fixar o conector de

¹⁹ “Appropriate anti-contamination precautions should be taken to minimize any chance of accidental contamination of items, which may subsequently be required for other laboratory examinations, e.g. fingerprints, DNA.

²⁰ “It is also helpful to mark this location on a sketch/plan of the scene or person.”

²¹ Artigo disponível em <http://www.dpt.ba.gov.br/dpt/web/ICAPInterna.jsp?ModId=70>

força na parte posterior do computador²²”, bem como a “interromper todos os pontos de acesso (entradas e saídas de cabos) da máquina²³”. “Devem ser removidas as baterias do interior de *laptops*²⁴” (SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, 2006, tradução nossa).

Sampaio²⁵ adverte a necessidade de cuidados especiais no transporte, pois “discos rígidos não suportam golpes, mídias magnéticas podem apresentar perda de dados se submetidas a campos magnéticos, a superfície pode apresentar desgaste se exposta a calor, umidade e poeira”. E ainda prossegue ressaltando a necessidade de se manter distância de fontes emissoras de ondas eletromagnéticas (celulares e rádios VHF) ou de campos magnéticos (caixas acústicas e ímãs). Finaliza consignando que o material não poderá se deslocar verticalmente nem horizontalmente no interior do veículo.

2.4 O EXAME

Quando o perito inicia o levantamento de um local de crime informático, se o computador estiver ligado, certamente não deverá desligá-lo de imediato. Nessa situação, “existem dados [...] sensíveis que merecem prioridade na coleta, como por exemplo, dados sobre conexões de rede, memória aleatória, processos, usuários online, arquivos abertos” (MILAGRE, 2008, p. 13). Oliveira, Guimarães e Geus (2002) estabelecem que essas análises são fundamentais para o sucesso dos trabalhos, pois são a única oportunidade de se coletar dados que não estarão mais disponíveis quando a máquina for novamente ligada. Durante essa análise, cabe a advertência de Rodrigues (2006, p.95), ou seja, “avaliar o caso, prevendo a possibilidade de prontamente desconectar o equipamento, se houver suspeita de manipulação remota, através de rede [...]”. Farmer e Venema (2007) ressaltam que a coleta de informações de sistemas em execução requer cuidado e planejamento, onde primeiro passo é isolar a máquina de outros usuários e da rede.

Após a análise “a quente” das informações, o momento mais delicado é o desligamento do computador, pois não há unanimidade entre os autores para tal procedimento. Trevenzoli (2006) avalia que deve-se, simplesmente, desconectar o computador da tomada de energia, para que não haja alterações de data e hora ocasionadas

²² “Place evidence tape over the power plug connector on the back of the computer.”

²³ “Computer case sealed with evidence tape over case access points and power connector.”

²⁴ “Also, remove batteries from laptops.”

²⁵ *Op. cit.*

pelo desligamento correto. Essa é a posição defendida por Oliveira, Guimarães e Geus (2002), com a qual seriam evitadas as chances de se executar um programa destrutivo, eventualmente acionado pelo desligamento convencional. Costa (2003, p.12), entretanto, adverte que “o desligamento de uma estação ou servidor por simples interrupção do fornecimento de energia [...] pode acarretar danos graves ao sistema e até inviabilizar sua inicialização.” O autor lembra, ainda, que no caso do sistema operacional Windows, existe a opção “hibernar”, na qual é gravado o conteúdo da memória “de forma que, ao se religar o sistema, volta-se à condição anterior ao desligamento [...]”. O Scientific Working Group on Digital Evidence (SWGDE) é taxativo ao afirmar que “se o desligamento for necessário, use os comandos apropriados²⁶” (2006, p.4, tradução nossa) e consigna uma severa “advertência: puxar o plugue da tomada pode danificar seriamente o sistema, prejudicar itens legítimos e criar responsabilidades ao encarregado e ao departamento²⁷”.

Se por um lado computador ligado não deve ser desligado, por outro: “se o computador estiver desligado, *não* ligue o computador²⁸” (SWGDE, p.3, tradução nossa). Isso porque “uma inicialização não controlada pode comprometer os dados, o ordenamento seqüencial das evidências e uma efetiva caracterização das provas” (COSTA, 2003, p.15). Segundo Trevenzoli (2006), a inicialização do computador deverá ser feita com uma ferramenta que permita sua realização a partir de uma mídia como *cd-rom*, por exemplo.

Antes de se iniciar o exame propriamente dito, chega-se, segundo Costa (2003), ao ponto mais importante a ser observado numa análise computacional: a duplicação da mídia para o exame dos dados. Isto significa que “somente se não houver possibilidade de se evitar o exame direto no material de prova [...] é que o exame deve ser feito direito nas mídias de prova, caso contrário, devem ser duplicadas e os exames efetuados nas mídias de destino” (COSTA, 2003, p.25). Prossegue o mesmo autor explicando que esse processo de duplicação bit-a-bit permite a preservação integral de todo o conteúdo da mídia. Scudere (2006) coloca que as pesquisas na cópia preservam a integridade física e digital dos dados, permitindo futuras análises e resguardando o material de incidentes. Ademais, lembra que os dados analisados podem ser contestados pelas partes, e estas deverão ter as mesmas condições de acesso às cópias para realização de eventuais “contraprovas”. Costa (2003) finaliza a questão

²⁶ “If shutdown is necessary, use the appropriate commands.”

²⁷ “Warning: Pulling the plug could severely damage the system; disrupt legitimate business; and/or create officer and department liability.”

²⁸ “If the computer is turned off, *do not* turn on the computer.”

indo além, consignando ser altamente recomendável que se faça mais de uma cópia da mídia de provas, a fim de que os exames possam ser feitos com mais liberdade e segurança.

Essa duplicação pericial deve ser feita de maneira segura, utilizando-se um dispositivo de bloqueio de escrita em disco (Scudere, 2006), visando à integralidade dos dados. Após a realização da cópia, Trevenzoli (2006) assevera que deverá ser executado um algoritmo de *hash* (soma de verificação atribuída a um arquivo) para comprovação da integridade dos dados. Assim, o *hash* de um arquivo da mídia de provas deve ser o mesmo do arquivo copiado para a mídia de destino, garantindo que está íntegro e não sofreu alterações. Portanto, de acordo com Costa (2003), tem-se uma identificação única que pode ser verificada a qualquer momento. Tais *hashes*, obviamente, deverão ser armazenados (OLIVEIRA, GUIMARÃES, GEUS, 2002) e é recomendável, segundo Trevenzoli (2006) que todo o material seja guardado em local seguro, com acesso restrito, até que, de acordo com Scudere (2006), o caso seja totalmente encerrado.

Além da preservação da mídia de prova, Costa (2003, p.26) chama a atenção para o estabelecimento da cronologia dos eventos relacionados ao caso, a chamada linha de tempo ou *timeline*, que “pode mostrar toda a evolução de um caso” e ser “de grande utilidade para demonstrar a premeditação, organização e metodologia utilizada [...]”. O exame diretamente na mídia de prova alteraria todas as características que permitem estabelecer a *timeline* de um arquivo como, por exemplo, data de criação e última alteração. O perito ainda deverá estar extremamente atento para a advertência de Scudere (2006, p.221), pois “arquivos [...] podem ter [...] alterados os horários de criação, manipulação, envio/recebimento, entre outros” e “tais violações de arquivos e registros de logs tornam o processo de investigação [ainda mais] complexo”. Como existe a possibilidade de armadilhas montadas por invasores, Farmer e Venema (2007) consignam que o perito deve examinar cuidadosamente fragmentos de dados disponíveis, procurando inconsistências que demonstrem uma tentativa oculta de destruição de vestígios.

No momento da análise, outro cuidado a ser tomado diz respeito à escolha adequada dos programas e ferramentas a serem utilizadas pelo perito. Oliveira, Guimarães e Geus (2002) lembram que não é seguro utilizar softwares instalados na própria máquina. De acordo com Trevenzoli (2006), devem ser empregadas apenas ferramentas do próprio perito e não as que porventura existam na mídia a ser analisada, pois estas podem estar alteradas. Prossegue a autora ao consignar que não se “deve utilizar ferramentas que possam alterar as datas de último acesso dos arquivos existentes” (TREVENZOLI, 2006, p. 36). Nas palavras

de Oliveira, Guimarães e Geus (2002), as ferramentas devem fornecer “resultados relevantes causando o mínimo de distorção possível no sistema analisado.” Para a maximização do valor da prova, Scudere (2006) vai além e consigna que os programas de análise devem ser aceitos pelas organizações internacionais. Já para Sampaio²⁹, os softwares “deverão ser homologados pelo mercado ou por instituição voltada para o trabalho pericial e/ou jurídico [...]”

Quando se fala em “coletar dados” em uma análise informática, deve-se ter em mente que algumas informações “desaparecem” ou se alteram mais rapidamente que outras. Assim, a metodologia utilizada na coleta deve respeitar a chamada ordem de volatilidade, o que ocasiona maior probabilidade de serem preservados os detalhes mais efêmeros (FARMER e VENEMA, 2007). Nas palavras de Trevenzoli (2006, p.35), “caso essa ordem não seja seguida, algumas provas podem ser perdidas, pois uma ação fora de ordem pode alterar ou até apagar [...] registros”. Uma das justificativas para se observar a ordem de volatilidade reside no Princípio da Incerteza de Heisenberg³⁰, aqui explicado por Milagre (2008, p.13): “é impossível periciar um sistema sem afetá-lo em algum outro ponto. Periciar uma área de um sistema implica em alterações em outra área do mesmo.” Portanto, quando se procede a uma coleta de dados, alguns tipos de dados são mais propensos a sofrerem alterações do que outros (FARMER e VENEMA, 2007). Isso obriga o perito a estabelecer pontos-chave e identificar prioridades (OLIVEIRA; GUIMARÃES; GEUS, 2002).

Finalmente, resta consignar alguns lembretes aos peritos em informática, os quais, poderia se dizer, devem traduzir o “espírito” dos exames e são consignados por Farmer e Venema (2007). É impossível recuperar e analisar todos os dados de um computador. Dessa forma, como já dito, devem ser identificadas prioridades. Assim, talvez o perito deva “arriscar” a não obter alguns vestígios, em detrimento de outros, o que, segundo os autores, facultaria a possibilidade de se recuperar dados adicionais e de entender o problema como um todo. Finalizam consignando que nenhum dado deve ser considerado pontualmente, isoladamente. “Somente correlacionando os dados a partir de muitos pontos”, pode-se “começar a ter um bom entendimento do que aconteceu” (FARMER E VENEMA, 2007, p.173)

O trabalho do perito culmina com a elaboração do laudo pericial, no qual deve ser utilizada linguagem técnica, mas acessível, sem excessos, seguindo recomendações de normas

²⁹ *Op. cit.*

³⁰ Werner Karl Heisenberg – físico alemão formulador do Princípio da Incerteza, que afirma que ao conhecermos muito precisamente a posição de uma partícula, será muito grande a imprecisão sobre o valor de sua velocidade, sendo impossível conhecer as duas grandezas de maneira infinitamente precisa.

técnicas apropriadas. Deverá ainda informar toda a metodologia utilizada, técnicas empregadas, incluindo programas e materiais (SAMPAIO³¹). Entretanto, é muito bem ressaltado por Milagre (2008, p.44) que “somente técnica não é suficiente, mas a análise estratégica e lógica das informações colhidas.” Portanto, menciona, ainda, o autor que o perito deverá explicar “conclusões cronológicas sobre o que ocorreu [...], ou seja, “a reconstrução” do evento. Por fim, ao elaborá-lo, o perito só deve fazer afirmações que possam ser provadas e demonstradas, sobre as quais baseará sua conclusão. Quando não dispuser de meios para fundamentar uma conclusão, deve apenas consignar quais os dados obtidos, por seu compromisso com a verdade (TOCCHETTO, 2006).

3 CONCLUSÃO

A maximização do valor de uma prova obtida em meios eletrônicos no sistema processual brasileiro permeia os diversos momentos do exame pericial, até mesmo antes de seu início, quando da emissão da requisição de exame ou mandado judicial. Embora tais exames possam se levados a termo em uma infinidade de mídias e sistemas operacionais diferentes, os órgãos competentes não devem medir esforços em busca de uma padronização de procedimentos, o que tornaria menos viável um questionamento, pelas partes, dos resultados apresentados (OLIVEIRA; GUIMARÃES; GEUS, 2002). Portanto, o emprego de uma metodologia correta garante a aplicação da cadeia de custódia, preservando e documentando a evidência desde seu encontro, coleta, manuseio, transporte e análise.

O exame pericial deve, ainda, empregar o método científico, o que implica dizer que, segundo Oliveira, Guimarães e Geus (2002), os procedimentos utilizados devem ser reconhecidos pela comunidade científica e gerar resultados que possam ser reproduzidos, já que, o conteúdo de um Laudo Pericial deve ser invariante com relação do perito que o produziu e constante em relação ao tempo (DOREA; STUMVOLL; QUINTELA, 2006).

Finalmente, os peritos criminais devem dignificar seu trabalho, buscando aprimoramento contínuo em virtude da espantosa velocidade da informática. Assim, nas palavras de Tocchetto (2006), estarão oferecendo laudos mais fundamentados, minuciosos e confiáveis, de forma a tornar os processos mais céleres e as sentenças, mais justas.

³¹ *Op. cit.*

4 REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. *Código de Processo Penal*: Decreto-lei n.º 3.689 de 3-10-1941, atualizado e acompanhado de legislação complementar, súmulas e índices. 9.ª ed. São Paulo: Saraiva, 2003.

BRASIL. *Código Penal*. Decreto-lei n.º 2.848 de 7-12-1940, atualizado e acompanhado de legislação complementar, súmulas e índices. 9.ª ed. São Paulo: Saraiva, 2003.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Lei n.º 9.605, de 12 de fevereiro de 1998*. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L9605.htm>. Acesso em 04.07.2008.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. *Lei n.º 11.343, de 23 de agosto de 2006*. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2006/Lei/L11343.htm>. Acesso em 04.07.2008.

COSTA, Marcelo Antonio Sampaio Lemos. *Computação Forense*. 2.ª ed. Campinas: Millennium Editora, 2003. 246p. (Tratado de Perícias Criminalísticas, v. 9)

DOREA, Luiz Eduardo Carvalho; STUMVOLL, Victor Paulo; QUINTELA, Victor. *Criminalística*. 3.ª ed. Campinas: Millennium Editora, 2006. p. 60-80 (Tratado de Perícias Criminalísticas, v. 1)

ESPINDULA, Alberi. *Perícia Criminal e Cível: Uma visão geral para peritos e usuários da perícia*. 2.ª ed. Campinas: Millennium Editora, 2006. 442p.

FARMER, Dan; VENEMA, Wietse. *Perícia Forense Computacional: Teoria e Prática Aplicada*. Tradução de Edson Furmankiewicz e Carlos Schafranski. São Paulo: Pearson Prentice Hall, 2007. 190p.

INTERNATIONAL ORGANIZATION ON COMPUTER EVIDENCE. *Guidelines for Best Practice in The Forensic Examination of Digital Technology*. 2002. 24p. Disponível em: <http://www.ioce.org/fileadmin/user_upload/2002/ioce_bp_exam_dig_tech.html> Acesso em 18.06.2008.

MAGNO, Alexandre. *Das Perícias em Geral*. [S.L.], 2005. Disponível em <http://www.alexandremagno.com/read.php?n_id=101>. Acesso em 02.07.2008

MILAGRE, José Antonio Maurílio Milagre. *Perícia Eletrônica*. Dourados: UNIGRAN, 2008. 48p.

OLIVEIRA, Flávio de Souza; GUIMARÃES, Célio Cardoso; GEUS, Paulo Lício de. *Resposta a Incidentes para Ambientes Corporativos Baseados em Windows*. [S.L.]. 2002. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2002-WSeg-flavio.oliveira-resposta.incidentes.pdf>.> Acesso em 20.07.2008.

REIS, Alexandre Cebrian Araújo; GONÇALVES, Victor Eduardo Rios. *Processo Penal: Parte Geral*. 9.^a ed. rev. e atual. São Paulo: Saraiva, 2005. p. 116-126 (Coleção Sinopses Jurídicas, v. 14).

RESINA, Jane. Desmistificação da Internet para Advogados. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. (Org.) *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006.

RODITI, Itzhak. *Dicionário Houaiss de Física*. Rio de Janeiro: Objetiva, 2005. p.183.

RODRIGUES, Jorilson da Silva. Aspectos Práticos dos Crimes Informáticos. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. (Org.) *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006.

SAMPAIO, Marcelo. *Normas e Procedimentos para a Computação Forense*. Disponível em <<http://www.dpt.ba.gov.br/dpt/web/ICAPInterna.jsp?ModId=70>> Acesso em 15.07.2008.

SÃO PAULO. Polícia Civil do Estado de São Paulo. *Manual de Polícia Judiciária, doutrina, modelos, legislação*. São Paulo: Delegacia Geral de Polícia, 2000.

SÃO PAULO. Polícia Civil do Estado de São Paulo. *Manual Operacional do Policial Civil, doutrina, legislação, modelos*. São Paulo: Delegacia Geral de Polícia, 2002.

SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. *Best Practices for Computer Forensics*. 2006. 11p. Disponível em <http://www.swgde.org/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf> Acesso em 20.07.2008.

SCUDERE, Leonardo. Análise Forense – Tecnologia. In: BLUM, Renato M. S. Opice; BRUNO, Marcos Gomes da Silva; ABRUSIO, Juliana Canha. (Org.) *Manual de Direito Eletrônico e Internet*. São Paulo: Lex Editora, 2006.

TOCCHETTO, Domingos. *Balística Forense: Aspectos Técnicos e Jurídicos*. 4.^a ed. Campinas: Millennium Editora, 2006. VII. (Tratado de Perícias Criminalísticas, v. 4)

TREVENZOLI, Ana Cristina. *Perícia Forense Computacional – Ataques, Identificação de Autoria, Leis e Medidas Preventivas*. 2006. 89f. Monografia (Trabalho de Conclusão de Curso) – Faculdades SENAC, Sorocaba. Disponível em <http://www.datasecur.com.br/academico/Pericia_Forense_Computacional_ataques.pdf> Acesso em 22.07.2008.

ZARZUELA, José Lopes. *A Prova Pericial no Foro Penal*. Revista da Faculdade de Direito da Universidade de São Paulo. [S.L.], v.90, p.303-315, jan./dez.1995.