Protocolo para execução de mandato de busca e apreensão em cenários de crimes digitais

Edson J. R. Justino*, Luiz E. S. de Oliveira**

1 INTRODUÇÃO

Com a evolução vertiginosa das telecomunicações e da computação, observou-se um crescimento significativo no uso das tecnologias propiciadas pelas duas áreas. Empresas, governos e sociedade passaram a fazer uso intensivo desses recursos. No entanto, observou-se também, nas mesmas proporções, o crescimento das atividades criminosas envolvendo essa mesma tecnologia. Crimes digitais ou cibernéticos que há algumas décadas atrás representavam uma pequena parcela dos crimes tratados pela Justiça, passaram a tomar proporções maiores e em algumas áreas, suplantaram os convencionais. Como exemplo pode-se citar os crimes envolvendo instituições financeiras e seus clientes, que no segundo semestre de 2005 tiveram um acréscimo de 1,04% para 1,45% (Relatório Vírus, 2006). Grupos bem organizados e com conhecimento tecnológico suficiente, passaram a atuar intensivamente na rede mundial de computadores em vários níveis. Os alvos de ataque são diversos: empresas, instituições financeira, pessoas físicas, agências governamentais, entre outras. No Brasil em 2005 os prejuízos chegaram a 300 milhões de reais (WNews, 2006) . As expectativas para os próximos anos é um crescimento ainda maior dessa modalidade de crime em dimensões globais (Departamento da Polícia Federal, 2006; Nancy Ritter, 2006).

Até o final da década de 90 o foco principal da Ciência da Computação, em especial a área de redes, era direcionado ao desenvolvimento de soluções para garantir a inviolabilidade dos ambientes computacionais. O objetivo até então era tratar dos eventos criminosos antes que os mesmo acontecessem. No entanto, a experiência mostrou que se trata de uma tarefa árdua e de difícil execução, em virtude da diversidade tecnológica e de rápidas mudanças impostas por essa mesma tecnologia. Dados estatísticos de 2005 demonstram que 69% da vulnerabilidade relatada no segundo semestre do mesmo ano, forma encontradas na Web (Relatório Vírus, 2006). Dentro desse novo cenário mundial, uma nova área se apresenta com o objetivo de contribuir com a minimização dos efeitos provocados pela ação criminosa, a Computação Forense.

A Computação Forense se apresenta como uma alternativa para atender os casos de pós-evento. Isto é, tratar a ação criminosa após sua execução. Sua principal característica esta na relação direta com as diferentes áreas do Direito (Criminal, Cível, Tributário, entre outras), uma vez que busca em evidências tecnológicas a materialização da prova que caracterizam a ação criminosa e as relaciona com as pessoas envolvidas.

A tecnologia digital incorporou novos conceitos que não podem ser tratados pela justiça, segundo a abordagem adotada nos processos tradicionais. O ambiente digital e sua tecnologia, modificaram drasticamente os conceitos de evidência e de prova. O ambiente digital traz consigo as características de volatilidade, alterabilidade e fácil falsificação (Marcacini, 2006), Tais características somadas à diversidade de ambientes computacionais e de tecnologia, dificultam a criação de metodologias que se sustentem, quando submetidos às argüições jurídicas ou às restrições legais.

No domínio da Computação Forense a solução de problemas complexos, tal como o apresentado, exige um largo espectro de conhecimento em áreas afins (Computação, Telecomunicação, Ciência Forense e Direito) e também alguns mecanismos para a manipulação desse conhecimento. Para definir precisamente um problema na área em questão é necessário incluir especificações sobre qual será a situação e também sobre quais situações finais serão consideradas soluções aceitáveis. Portanto, a identificação e representação do conhecimento necessário para solucionar o problema, juntamente com a escolha das melhores técnicas a serem usadas, formam o conjunto de atribuições necessárias e suficientes para formalizar uma solução.

A Computação Forense incorpora inúmeras características que juntas, criam um ambiente favorável para a definição de um parecer ou opinião sobre uma determinada evidência. No entanto, tais evidências estão sujeitas, em sua grande maioria, às restrições impostas pelo meio digital, na forma de obtenção e na garantia de sua integridade. Assim sendo, a definição de metodologias para o rastreamento e obtenção de tais evidências, se torna uma tarefa delicada, em função da diversidade das mesmas, do cenário onde estão inseridas e das restrições legais envolvidas (Nancy Ritter, 2006).

A busca e apreensão é uma das etapas mais importante do processo de análise pericial criminal de material suspeito. É o resultado de longos períodos de investigação, onde se mobilizam recursos humanos e logísticos, a fim de coibir e punir as atividades criminosas. O objetivo desse artigo é propor um protocolo para a execução de busca e apreensão em cenários de crimes digitais. Para tanto, esse artigo foi dividido em 6 tópicos a saber. O primeiro contém essa breve descrição. O segundo descreve os conceitos de evidência, sobre a ótica da Ciência Forense. O terceiro descreve os cenários de crimes digitais e suas características. O quarto apresenta uma visão geral sobre os artigos que regem a busca e a apreensão no Código de Processo Penal Brasileiro. O quinto tópico apresenta o protocolo proposto. O sexto e último tópico são apresentadas as considerações finais e propostas para trabalhos futuros.

2 EVIDÊNCIA

Em Ciência Forense o valor de uma evidência é medida por quatro parâmetros, a saber: (William G. Eckert, 1997)

- A relevância, que descreve a importância da evidência no contexto ou escopo dos fatos ocorridos;

- A materialidade, que descreve capacidade da evidência em ajudar a reproduzir os fatos ocorridos;

- A credibilidade, que descreve o meio pelo qual a evidência foi obtida;

- A Competência, que descreve o nível de validade dos procedimentos científicos empregados na análise e teste da mesma.

Em um cenário de crime digital é possível encontrar dois tipos básicos de evidências, as físicas e as demonstrativas (FBI, 2003). As físicas são obtidas na cena do crime e devem receber os mesmos cuidados dedicados a outras classes de evidência, tais como impressões digitais, DNA. Esses cuidados decorrem da facilidade de contaminação ou da destruição da mesma. Em Computação Forense, a contaminação usualmente ocorrer quando existe o acesso e a manipulação da evidência por pessoas não autorizadas, na cena do crime ou fora dela. A destruição ocorre quando existe a manipulação incorreta das mesmas usualmente na cena do crime, desconectando cabos de rede com o equipamento ligado, desligando o equipamento sem a prévia análise, entre outros.

As evidências demonstrativas são usualmente produzidas a partir da evidência física e por essa razão, o cuidado com a integridade física da mesma é de fundamental importância. Entre as várias evidências físicas encontradas em cenários de crimes digitais, destacam-se: os computadores e seus periféricos, equipamentos de conectividade, documentos e suprimentos.

Usualmente, a busca por evidências demonstrativas, a partir das físicas, ocorre no Laboratório Forense, onde estão disponíveis equipamentos e software adequados para garantir a materialidade, integridade e credibilidade das mesmas (Joseph C. Sremack, 2004). Em alguns casos, onde o equipamento encontra-se em operação, ou não puder ser removido para o Laboratório, a coleta de evidências demonstrativas pode ocorrer na cena do crime.

3 CENÁRIO DE CRIME

Em Ciência Forense um cenário de crime é geralmente um local onde um crime ocorreu, ou um local onde um incidente criminoso iniciou-se, ou concluiu-se. O cenário pode ser dividido em duas classes (John Horswell, 2004):

- Cenário primário ou cena preliminar do crime. É uma área ou local onde o incidente ocorreu, ou onde a maioria ou uma concentração elevada da evidência física serão encontradas. Como exemplo, pode-se citar: CDROM, computadores, modem, entre outros;

- Cenário secundário do crime é um ou mais lugares ou objetos onde existem evidências físicas ou demonstrativas que se relacionam ao incidente. Por exemplo, equipamento atingido pelo evento de invasão.

Numa diligência ou busca, na maioria das vezes, evidências encontradas em cenários distintos, se completam a fim de proporcionar a reconstrução do evento criminoso, ou

associar o suspeito ao ato criminoso. Num processo de invasão, por exemplo, parte das evidências pode ser encontrada no cenário primário (origem da invasão) e no cenário secundário (alvo da invasão).

Uma diligência bem sucedida, em um cenário de crime digital, é determinada pelos resultados obtidos. Um investigador de cenário de crimes digitais deve identificar, coletar e utilizar cada parte das evidências físicas ou demonstrativas que puder encontrar. Evidências valiosas podem estar escondidas entre inúmeros materiais sem valor aparente.

Para que uma diligência seja bem sucedida as seguintes questões devem ser respondidas (FBI, 2003):

- Qual é o tipo da evidência, física ou demonstrativa?

- Como gravar, coletar e preservar?

- Como obter dele a informação que carrega?

- Como interpretar a informação obtida?

- Como garantir sua integridade e autenticidade?

As respostas a essas questões podem ser respondidas em parte diante da cena do crime, observando um protocolo rígido de coleta. A outra parte pode ser respondida pelo Cientista Forense, em Laboratório, através de procedimentos padronizados de análise.

4 MANDATO DE BUSCA E APREENSÃO

O Estado brasileiro vem provendo os mecanismos preventivos e repressivos de práticas ilícitas, na esfera civil e penal, bem como vem incentivando a organização de setores especializados no combate à criminalidade digital. Polícia Judiciária, Ministério Público, Polícia Federal, estão sendo mobilizados a fim de atender a demanda crescente de crimes de natureza digital.

Dada a natureza do delito e do alto grau de lesividade, certas condutas que atentam contra bens informáticos ou informatizados, ou em que o agente se utilize do computador para alcançar outros fins ilícitos, devem ser penalizados criminalmente (Vladimir Aras, 2006).

Nesse contexto, uma das ferramentas importante para o combate ao crime digital encontra-se o mandato de busca e apreensão. Esse instrumento propicia a legitimidade necessária na busca de evidências que provem o ato criminoso e a associação com seus autores.

O mandato de busca e apreensão é o meio de prova que consiste na apreensão de pessoas ou objetos, cuja natureza contribua para elucidação do crime. A busca será domiciliar ou pessoal (Marcela M. R. de Vasconcellos, 2006).

O mandato de busca e apreensão, segundo o Código de Processo Penal Brasileiro (CPP, 1996), artigo 240 a 250, determina que a busca e apreensão deva ser realizada por autoridade policial e judiciária. Essa busca poderá ser determinada a requerimento de qualquer das partes ou de ofício.
Acabadas as diligências, os executores lavrarão auto circunstanciado, assinando-o com duas testemunhas presenciais.

Apesar dos esforços dos órgãos competentes, inexiste no Brasil uma padronização a seca do protocolo a ser utilizado na execução de um mandato de busca e apreensão em crimes digitais. A falta de padronização ou de um protocolo adequado pode invalidar meses ou até anos de investigação.

5 PORTOCOLO PROPOSTO

O protocolo proposto se baseia nos princípios da análise de cenários de crimes em Ciência Forense, que possui como meta resguardar a integridade, credibilidade, materialidade, relevância e competências das evidências encontradas em cenas de crimes digitais. O protocolo proposto se divide em sete etapas a serem descritas a seguir.

5.1 Preparativos

A preparação da diligência deve ser discutida pelo pessoal envolvido. Devem-se definir, com antecedência, os papeis a serem assumidos pelo pessoal envolvido, de acordo com suas aptidões. O passo seguinte é estabelecer uma hierarquia para responder aos contingenciamentos que venham a surgir no cenário principal e secundário, Deve-se assegurar que todas as pessoas envolvidas estejam cientes das atividades a serem executadas, dos tipos de evidências a serem procuradas e da forma mais adequada para a manipulação das mesmas. As atividades devem ser distribuídas a dois ou mais responsáveis, a redundância garante a qualidade do processo de busca (John Horswell, 2004).

É possível que, em alguns casos, o mandato seja restritivo para algum tipo específico de evidência. Nesse caso, cuidados adicionais devem ser tomados a fim de evitar a impugnação das mesmas. Ocorrências desse tipo são comuns quando envolvem informações de terceiros.

5.2 Abordagem Inicial do Cenário

A avaliação das possibilidades físicas de uma evidência começa ao adentrar o cenário do crime e se torna detalhada nas etapas subseqüentes. É necessário assegura que o material coletado será perfeitamente acondicionado e que os registros ou documentação serão feitos de forma adequada.

As evidências demonstrativas, tais como: configurações, arquivos de swap, dumps de memória, entre outros, devem ter prioridade sobre as demais evidências. Essa classe de evidência pode desaparecer, ou ser de difícil recuperação, se não for tratada no momento oportuno (Brian Carrier, 2005). É importante salientar que somente nos casos em que o

equipamento esteja ligado, esse procedimento se faz necessário. Em nenhuma hipótese, qualquer equipamento encontrado no cenário de crime deve ser ligado no local.

Durante o processo de busca, deve-se proibir a entrada de pessoas não autorizadas no cenário, esse procedimento evita a contaminação e a destruição de evidências. Como exemplo pode-se citar, casos em que durante o processo de busca e apreensão, foram registradas imagens de pessoas não autorizadas junto às evidências, desqualificando sua integridade.

5.3 Busca de Evidência no Cenário

O registro físico das evidências pode ser obtido utilizando-se os padrões de busca definidos pela Ciência Forense para a análise de cenários de crimes. Os padrões são (FBI, 2003):

- Grade ou gride consiste na segmentação da área da cena em setores ou retângulos, onde se procederá ao processo de busca, confira na fig. 1b;

- Varredura consiste na busca linear das provas em toda a extensão da cena, confira na fig. 1c;

- Espiral consiste numa busca partindo-se do extremo do ambiente, dirigindo-se ao centro da cena, confira na fig. 1d.

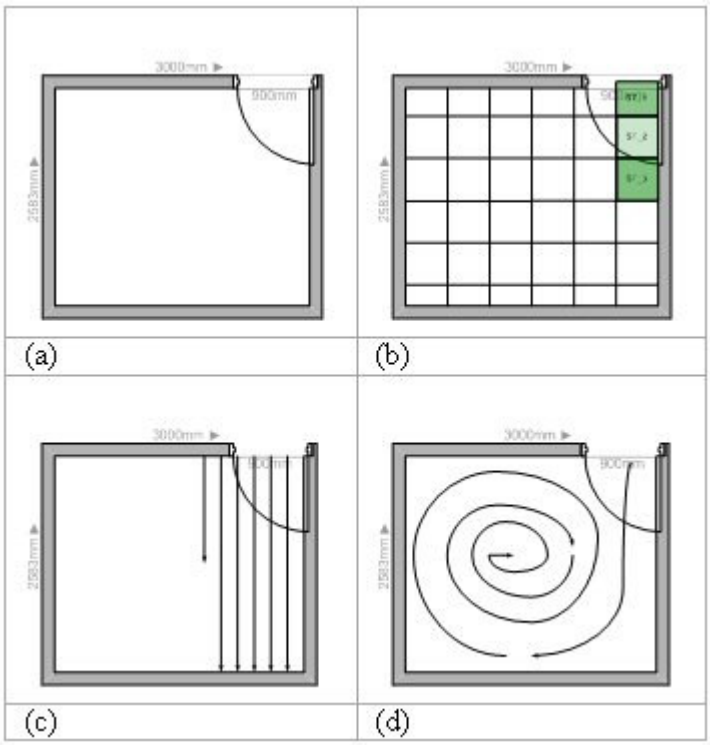

Fig. 1 – Padrões de busca em cenários de crimes. (a) Cenário do crime digital; (b) Busca em grade; (c) Busca em varredura; (d) Busca em Espiral.

Numa busca preliminar as evidências devem ser rotuladas com um marcador, usualmente uma plaqueta contendo um número, que deve ficar próximo da mesma, para facilitar sua localização e registro. A busca por evidências deve ocorrer sempre do geral para o específico. O material colhido deve ser fotografado antes de ser removido do seu local de origem. O material colhido deve ser incluído no registro de evidências juntamente com a numeração das fotos, confira na tabela 1. O registro fotográfico facilita o trabalho de construção do laudo pericial.

Tabela 1 - Registro de evidências

Registro de Evidências			
Data: __/__/____		Processo:	
Horário de Entrada:		Data :__/__/____ Horário da Liberação:	
Evidência	Descrição	Fotos	V
EF_1	*Caixa de CDROM*	*1, 2, 3, 4*	٢
EF_2	*Disco SCASI No. 234578945678*	*5,6,7,8*	٢
...	*...*	*...*	*..*
EF_10	*Lixeira*	*34,35,36*	٢
Padrão de Busca: *Espiral*			
Nome do Fotógrafo:			
Responsável:			

Testemunha:
Testemunha:

Uma das ferramentas mais importante a serem utilizadas ao abordar a cena do crime, pela primeira vez, é o descritivo físico do cenário (FBI, 2003). O esquema ou esboço pode ser feito inicialmente a mão livre e posteriormente, transcrito utilizando-se uma ferramenta apropriada. O esboço estabelece um registro permanente das evidências físicas e em que circunstâncias as mesmas foram encontradas. O esboço suplementa as fotografias e o registro de evidências. O importante nessa etapa é observar todos os detalhes do ambiente e registrar, através de desenho e fotografias, todo o cenário e seus componentes. Um exemplo pode ser visto na Fig. 3.

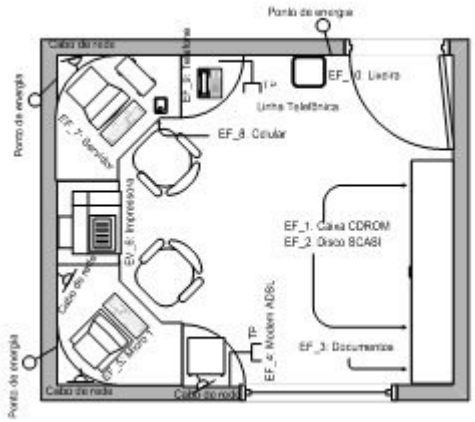

Fig. 3- Exemplo de descritivo físico de um cenário de crime.

Na Fig. 3 é possível observar a identificação de todas as evidências físicas encontradas na cena. Cada qual recebe um código de identificação (ID) (EF_ número). Esse ID será utilizado sempre que a evidência for referenciada. É bom salientar que outras evidências físicas podem derivar das já cadastradas na cena do crime. Como exemplo pode-se citar as unidades de disco encontras em um computador. A manipulação e novos registros devem ser feitos no Laboratório Forense, a fim de evitar que ocorram danos decorrentes de acidentes ou do manuseio impróprio.

5.4 Fotografias

O cenário do crime deve ser fotografado o mais cedo possível, de preferência após a rotulação das evidências. Estabelece uma progressão de vistas totais, médias, e do close-up

da cena de crime. É necessário fotografar as condições da evidência antes da retirada do local. No registro de evidências inclua o nome do fotografo.

5.5 Manipulação de Evidências

O mais importante é manusear a evidencia o menos possível. Assim que os registros das mesmas forem feitos, devem ser acondicionadas adequadamente e retiradas da cena. Alguns cuidados adicionais devem ser tomados com os equipamentos que possuam recursos de armazenamento removíveis, tais como computadores, câmeras fotográficas, entre outros. Esses equipamentos devem ter suas vias de acesso aos dispositivos de armazenamento lacrados, a fim de evitar a contaminação, isto é, que os mesmo sejam retirados ou manuseados sem autorização. No caso específico dos computadores, deve-se colocar um lacre nas vias de acesso interno e também nas entradas de energia. O uso do lacre garante a integridade da prova até a chegada ao Laboratório. O lacre pode ser feito com uma etiqueta de identificação, contendo o ID da evidência, o número do caso e a rubrica do responsável pelo lacre.

Quando as evidências a serem recolhidas forem pequenas, tais como disquetes, cds, discos rígidos, entre outros, o material deve ser acondicionado em pacotes e os mesmos devem ser lacrados e etiquetados, como descrito anteriormente. O material deve ser obrigatoriamente selado na cena do crime (John Horswell, 2004). O uso de sacos plásticos não é indicado nesses casos. O material quando mantido lacrado por longo tempo, pode adquirir fungos e deteriorar rapidamente. A mesma regra se aplica aos computadores.

5.6 Exame Final da Cena

O exame final é uma revisão de todos os aspectos da busca. Deve ser feita uma revisão com todos os envolvidos no processo, a fim de determinar se toda a documentação está correta e completa. Assegurar de que todas as evidências foram catalogadas. Assegurar de que locais de difícil acesso ou escondidos não foram negligenciados. O registro de evidências deve ser revisto e confirmado, o campo (V) do registro de evidências deve ser usado nessa fase, para indicar que o processo foi concluído (FBI, 2003).

5.7 Liberação da Cena

A liberação da cena, após o exame final, é composta pelo registro de evidências, contendo a data e hora da liberação (William G. Eckert, 1997). Nessa etapa a importante assegurar que todas as evidências foram recolhidas.

Como rege o Código de Processo Penal Brasileiro, artigo 245, inciso sete, finda a diligência, os executores lavrarão auto circunstanciado, assinando-o com duas testemunhas presenciais. As mesmas testemunhas irão assinar o registro de evidências no campo apropriado.

6 CONCLUSÃO

Esse artigo apresentou um protocolo para a execução de mandatos de busca e apreensão em cenários de crimes digitais. O protocolo propõe um padrão com abordagem prática para a execução de diligências, segundo os paradigmas de qualidade definidos para a Ciência Forense. O objetivo principal é reduzir os incidentes decorrentes da não observância dos requisitos impostos pela legislação, no que se refere ao trato de evidências digitais e da manutenção de sua integridade.

A proposta para trabalhos futuros é desenvolver um protocolo para o tratamento de evidências demonstrativas em laboratório e em campo, isto é, no cenário de crime. Esse segundo trabalho levará em consideração as ferramentas de código aberto (open source), a fim de estabelecer a credibilidade científica e legal às ferramentas utilizadas para este fim.

AGRADECIMENTOS

Os autores agradecem o apoio financeiro do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) que vem apoiando as iniciativas nessa área estratégica para o Brasil.

Referências bibliográficas

ECKERT, William G.. **Introduction to Forensic Sciences**. CRC Press, 2nd edition, USA, 1997, p. 385.

FBI, Federal Bureau of Investigation. **Handbook of Forensic Science, U. S. Department of Justice, USA**, 2003, p. 130.

SREMACK, Joseph C.. **Formalizing Computer Forensic Analysis**: A Proof-Based Methodology. Thesis submitted to the Graduate Faculty of North Carolina State University for the Degree of Master of Science Department of Computer Science, Raleigh, of North Carolina, USA, 2004, p. 127.

HORSWELL, John. **The Practice of Crime Scene Investigation**. International Forensics Science and Investigation Series, CRC Press, USA, 2004, p. 424.

CARRIER, Brian**. File System Forensic Analysis**. Addison Wesley Professional, 2005, USA, p.600.

CPP. **Código de Processo Penal**. Ed. Saraiva, 36ª. Edição, São Paulo , SP, Brasil, 1996,p. 629.

RITTER, Nancy. **Digital Evidence**: How Law Enforcement Can Level the Playing Field With Criminals. NIJ - Journal of National Institute of Justice, USA, no. 154, july, 2006, http://www.ojp.usdoj.gov/nij/journals/254/digital_evidence.html, acesso em 15/08/2006.

RELATÓRIO,vírus. **Crimes pela Internet viram Atividade Lucrativa**. Terra, Brasil, http://tecnologia.terra.com.br/interna/0,,OI929866-EI4805,00.html, acesso em 10/08/2006

WNEWS, Internet. Crimes digitais geraram prejuízo de R$ 300 mi em 2005. **UOL**, Brasil, http://wnews.uol.com.br/site/noticias/materia.php?id_secao=4&id_conteudo=4148, acesso em 15/08/2006.

VASCONCELLOS, Marcela Montanari Ramos de. **Busca e Apreensão**. http://www.pailegal.net, acesso em 07/08/2006.

ARAS, Vladimir. **Crimes de informática**. Uma nova criminalidade. http://jus2.uol.com.br/doutrina/texto.asp?id=2250. acesso em 14/08/2006.

*Edson J. R. Justino. Grupo de Pesquisa em Computação Forense e Biometria - Pontifícia Universidade Católica do Paraná - LabDOC – Laboratório de Documentoscopia

**Luiz E. S. de Oliveira. Laboratório de Computação Forense e Biometria Pontifícia Universidade Católica do Paraná - PUCPR Curitiba – PR

Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=1517..>Acesso em: 05 mar. 2008.