Investigação Digital: conceitos, ferramentas e estudos de caso

Evandro Della Vecchia Pereira
Instituto-Geral de Perícias/RS – Seção de Informática Forense
Universidade do Vale dos Sinos (UNISINOS)
Faculdade de Tecnologia SENAC-RS

***Resumo* — Com o crescente número de crimes virtuais surgiu a necessidade de uma investigação voltada ao meio digital. A legislação brasileira não possui leis específicas para este tipo de crime, porém é possível verificar que os crimes são basicamente os mesmos previstos no Código de Processo Penal (CPP), mas cometidos através do uso de computadores e similares. A idéia deste tutorial é mostrar um pouco do CPP ligados à perícia, alguns conceitos de forense digital, metodologias, ferramentas e alguns estudos de caso para que seja possível entender onde e como atua o profissional investigador ou perito digital.**

***Palavras-chave*—investigação digital, perícia digital, forense digital, crime cibernético, crime digital.**

I. INTRODUÇÃO

A cada ano que passa a quantidade de crimes aumenta de forma assustadora. E a tecnologia, que facilitou a vida de todos em várias tarefas, também ajudou no cometimento ou no armazenamento de dados destes crimes.

Diante disto, surgiu a necessidade da criação de delegacias especializadas e a demanda por peritos especializados na área de informática. Muitas vezes um perito é chamado de perito forense digital, o que nem sempre é verdade, pois um perito pode ser criminal, judicial ou contratado por uma empresa (particular). Porém o nome mais utilizado na literatura é *forense digital* (termo que será utilizado neste trabalho).

A ideia deste tutorial é mostrar um pouco da atividade do perito na área de informática, seja ele criminal, judicial, particular. Primeiramente serão mostrados alguns conceitos e um pouco de legislação referente à perícia, mostrando onde cada perito pode atuar. Após serão mostradas metodologias aplicadas na forense digital; ferramentas pagas e livres, incluindo distribuições Linux aplicadas à forense digital; e por fim estudos de caso para ilustrar situações reais.

II. CONCEITOS DE INVESTIGAÇÃO DIGITAL

A. *Legislação Brasileira*

O Brasil é regido por diversas leis que atendem particularmente cada necessidade. Nestas leis, como o Código Penal (CP), são descritos os direitos, obrigações e penas para todos os cidadãos brasileiros, salvo aqueles que possuem foro privilegiado. As questões relacionadas para o desenrolamento de crime tipificado pelo Código Penal são descritas no Código de Processo Penal (CPP) em vigor a partir da publicação do Decreto de Lei n.º 3.689, de 3 de Outubro de 1941. Dentre estas questões encontram-se os artigos relacionados à perícia criminal. A perícia criminal compreende as mais diversas áreas forenses, mas o foco desta seção é mostrar o conteúdo que pode ser relacionado à computação forense.

Um perito somente deve atuar caso seja solicitado, de nenhuma forma ele poderá realizar uma perícia baseado apenas em seu instinto. Caso isso ocorra o laudo apresentado não terá nenhum valor jurídico. Para que ele possa realizar uma perícia a autoridade policial ou o Ministério Público deve o requerer formalmente, conforme o Art. 6º:

> "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." [1]

O Art. 178 descreve que este requerimento deve ser entregue ao responsável pelo instituto de perícias que por sua vez encaminha para o perito da área solicitada. O artigo anteriormente comentado se relaciona com o Art. 159 que será comentado a seguir.

> "Art. 159 - O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior (alterado pela Lei nº 11.690, de 09 de junho de 2008).
> § 1º - Não havendo peritos oficiais, o exame será realizado por duas pessoas idôneas, portadoras de diploma de curso superior, escolhidas, de preferência, entre as que tiverem habilitação técnica relacionada à natureza do exame.
> § 2º - Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo."
> "Art. 178 - No caso do art. 159, o exame será requisitado pela autoridade ao diretor da repartição, juntando-se ao processo o laudo assinado pelos peritos." [1]

Além do perito não poder atuar de forma autônoma em uma perícia ele deve atender a alguns requisitos, conforme a

legislação. O preenchimento destes requisitos nada mais serve como uma proteção para que o laudo seja realizado com maior clareza e veracidade possível. O CPP traz em seu texto o que é necessário para ter as atribuições de um perito, mas quando inexiste este especialista na instituição estadual ou federal para alguma área em especifico, a escolha do perito fica a cargo do responsável do caso, o delegado ou promotor/juiz, que deve nomear algum profissional capacitado e com curso superior para tomar de posse das evidências e elaborar o laudo pericial. Este profissional, descrito no CPP como perito não oficial, precisa dominar o assunto do qual ele realizará a perícia, como descrito abaixo.

> "Art. 279 - Não poderão ser peritos:
> I -os que estiverem sujeitos à interdição de direito mencionada no Art. 47 do Código Penal;
> II - os que tiverem prestado depoimento no processo ou opinado anteriormente sobre o objeto da perícia;
> III - os analfabetos e os menores de 21 (vinte e um) anos" [1]

Os peritos, tanto os oficiais como os não-oficiais, são pessoas de confiança do juiz, conforme Art. 275. Por este motivo é necessário que o perito cumpra os prazos estabelecidos no CPP. Outro ponto importante está no Art. 277 que relaciona a obrigatoriedade do perito em realizar a atividade quando for escolhido pela autoridade. Caso ele não cumpra com as suas obrigações ou prejudique a perícia, este será enquadrado nos itens já descritos na legislação. O Art. 278 descreve inclusive a solicitação de prisão do perito caso ele não compareça sem justa causa. Pode ocorrer em alguns casos, de acordo com o Art. 105, de o perito ser excluído por solicitação de alguma da partes, mas esta deve argumentar e provar os motivos para o afastamento do profissional da atividade que será julgada pelo juiz. Toda essa preocupação também visa que o laudo final contenha os fatos realmente ocorridos [1].

> "Art. 275 - O perito, ainda quando não oficial, estará sujeito à disciplina judiciária.
> Art. 277 - O perito nomeado pela autoridade será obrigado a aceitar o encargo, sob pena de multa de cem a quinhentos mil-réis, salvo escusa atendível.
> Parágrafo único - Incorrerá na mesma multa o perito que, sem justa causa, provada imediatamente:
> a) deixar de acudir à intimação ou ao chamado da autoridade;
> b) não comparecer no dia e local designados para o exame;
> c) não der o laudo, ou concorrer para que a perícia não seja feita, nos prazos estabelecidos [BRASIL, 2004, p. 70].
> Art. 278 - No caso de não-comparecimento do perito, sem justa causa, a autoridade poderá determinar a sua condução." [1].
> "Art. 105 - As partes poderão também argüir de suspeitos os peritos, os intérpretes e os serventuários ou funcionários de justiça, decidindo o juiz de plano e sem recurso, à vista da matéria alegada e prova imediata." [1].

Por fim, a legislação deixa claro no Art. 160 que o objetivo final do perito é elaborar um laudo minucioso, sempre observando os prazos, explicando todos os detalhes da perícia realizada e das informações encontradas. Como descrito no Art. 159, o laudo deve ser elaborado por dois peritos, mas se houver divergências entre eles cada um deve elaborar um laudo em específico com as suas conclusões, atendendo assim o Art. 180. Pode também ocorrer de a autoridade, seguindo o Art. 181, solicitar novamente uma perícia para outros peritos, caso ele não se sinta confortável com o laudo inicialmente apresentado ou se os peritos não observarem as formalidades e deixaram obscuras as conclusões.

> "Art. 160 - Os peritos elaborarão o laudo pericial, onde descreverão minuciosamente o que examinarem, e responderão aos quesitos formulados.
> Parágrafo único - O laudo pericial será elaborado no prazo máximo de 10 (dez) dias, podendo este prazo ser prorrogado, em casos excepcionais, a requerimento dos peritos" [1].
> "Art. 180 - Se houver divergência entre os peritos, serão consignadas no auto do exame as declarações e respostas de um e de outro, ou cada um redigirá separadamente o seu laudo, e a autoridade nomeará um terceiro; se este divergir de ambos, a autoridade poderá mandar proceder a novo exame por outros peritos.
> Art. 181 - No caso de inobservância de formalidades, ou no caso de omissões, obscuridades ou contradições, a autoridade judiciária mandará suprir a formalidade, complementar ou esclarecer o laudo.
> Parágrafo único - A autoridade poderá também ordenar que se proceda a novo exame, por outros peritos, se julgar conveniente" [1].

Todas as formalidades relacionadas à perícia sempre devem ser levadas em consideração, pois como descrito o perito é uma pessoa de confiança do juiz sendo ela às vezes o fator decisivo para esclarecer um caso. A legislação vigente nos traz os itens anteriormente relacionados sobre todos os quesitos que o perito deve observar, tanto para preservar a perícia como a ele mesmo, pois nos casos onde houver má fé do perito este poderá pagar uma multa ou até ser preso caso se negue ou prejudique a realização da perícia [1].

No entanto, o juiz tem o livre-arbítrio para aceitar ou não a conclusão do laudo pericial, pois mesmo que o perito seja sua pessoa de confiança a legislação deixa claro que o julgamento final está ao entendimento do juiz. Este pode aceitar integralmente ou parcialmente o laudo apresentado conforme artigo a seguir.

> "Art. 182 - O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte." [1].

B. Etapas da Forense Digital

A Computação Forense faz parte de um processo investigativo, que tem com objetivo provar os fatos ocorridos com a maior clareza possível. Para que isso ocorra

o perito que for nomeado para realizar a perícia deve trabalhar de uma forma sistemática e cuidadosa com as evidências com o intuito de sempre preservar a integridade dos dados e detalhar toda a atividade executada no laudo final. Todo esse processo pericial na forense computacional é divido em quatro etapas conforme a seguir [2][3]:

- Coleta de dados: Esta etapa é considerada a mais vital de todo o processo, ou seja, a que mais precisa de cuidados. Ela tem tal importância, pois é nela que toda a massa crítica de dados será coletada, sendo necessário cuidado especial para manter a integridade das informações [4]. Outras atividades que são realizadas nesta etapa são relacionadas ao equipamento questionado, que deve ser identificado, devidamente embalado de uma forma segura, etiquetada as suas partes e suas identificações registradas no documento de cadeia de custódia [3];
- Exame dos dados: nesta segunda etapa o objetivo principal é separar as informações relevantes ao caso de outras sem importância, como os arquivos do próprio sistema. Antes de iniciar o processo é preciso definir quais as ferramentas que serão utilizadas para o exame dos dados. Esta escolha está relacionada a cada tipo de investigação e informações que estão sendo procuradas. Diante disso, pode se definir ferramentas que consigam trazer um número maior de dados úteis [2]. Peritos geralmente utilizam filtros de arquivos, busca por palavras-chave, entre outros procedimentos para agilizar a busca por evidências;
- Análise das Informações: na terceira fase, as informações anteriormente separadas serão analisadas com o intuito de encontrar dados úteis e relevantes que auxiliem na investigação do caso. Todos os dados encontrados considerados relevantes devem ser correlacionados com informações referentes à investigação, para que assim seja possível realizar a conclusão [3];
- Interpretação dos resultados: nesta última etapa, o objetivo é apresentar um laudo (relatório técnico) que deve informar com toda a veracidade possível o que foi encontrado nos dados analisados. Todo o processo pericial desde o início, ferramentas e informações que comprovem a integridade das informações devem ser relatadas no laudo [4].

De acordo com o descrito nas etapas anteriormente apresentadas, a Figura 2 demonstra de forma gráfica como é todo o processo de investigação em computação forense.

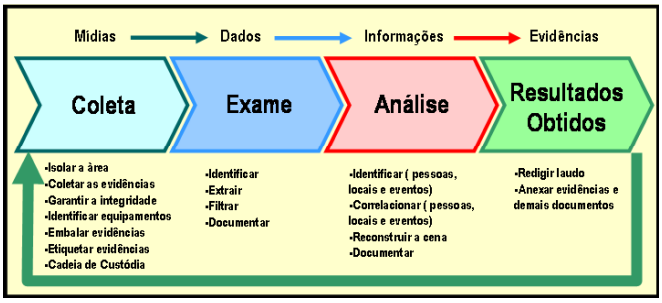

Figura 2: Fases do processo de investigação [3].

C. *Metodologias*

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: se a *Live Forensics* ou se a *Post Mortem Forensics*, ou, ainda, em alguns casos, se ambas [6][7].

A metodologia ***Live Forensics*** se caracteriza pela investigação do equipamento ainda em funcionamento. Esse método de trabalho é o único que permite a aquisição de informações voláteis, como por exemplo, os processos que estão sendo executados no computador, tabelas de roteamento, conexões estabelecidas, arquivos temporários, dados da memória principal, etc.

É extremamente importante que o perito tenha um conjunto de ferramentas próprias, testadas e homologadas, que não façam chamadas aos comandos nativos do sistema que está sob suspeita, a fim de evitar quaisquer danos causados por rootkits instalados no sistema.

A maior parte dos dados coletados do equipamento questionado pela metodologia *Live Forensics* são voláteis (com exceção de *logs* ou outros dados coletados do disco) e facilmente podem ser corrompidos ou destruídos, por isso é necessário o emprego de técnicas e ferramentas certificadas para a coleta, bem como a documentação de todo o processo.

Usada em maior escala, a metodologia ***Post Mortem Forensics*** é caracterizada pela análise realizada após o desligamento do equipamento questionado. Para isto, é recomendado é recomendado por boas práticas (não há lei que obrigue, no Brasil) a criação de uma cópia fiel (duplicação forense) do material questionado para uma posterior análise. Esta metodologia não requer tantos cuidados durante a aquisição de dados, se comparado com a *Live Forensics*, pois não há coleta de evidências voláteis. Apesar disto, é necessário validar a garantia de integridade dos dados por meio de funções *hash*.

A escolha da metodologia adequada vai depender do tipo de delito que será investigado. Por exemplo, em um suposto crime de pedofilia, onde arquivos de imagens gravados em disco são evidências, o perito fará uso da metodologia *Post Mortem Forensics*. Já para crimes de estelionato praticados por meios eletrônicos, poderão ser utilizadas as duas metodologias, a *Post Mortem Forensics* para a busca de dados que indiquem que o acusado tenha, por exemplo,

invadido o sistema de uma empresa, e a *Live Forensics* para averiguar conexões estabelecidas no instante da investigação.

III. FERRAMENTAS

As ferramentas são divididas em equipamentos e softwares. Em se tratando de software, existem aqueles reconhecidos mundialmente por órgãos policiais e/ou periciais, como o Encase [8] e o FTK [9]. Porém o custo desses softwares é muito alto. Em contrapartida existem softwares livre, incluindo distribuições Linux específicas para forense digital, com centenas de softwares para este fim. Alguns exemplos são: Helix [10], FDTK [11], PeriBR [12], entre outras. Além das distribuições Linux, existem também diversos softwares simples, cada um com seu objetivo restrito e específico, como por exemplo os softwares da Sysinternals (site criado em 1996 e adquirido pela Microsoft em 2006) [13].

Em se tratando de hardware, existem duplicadores forense, bloqueadores de escrita, aceleradores de descoberta de senha e cabos diversos, como podem ser vistos em *sites* como o do fabricante TABLEAU [14].

A ideia é apresentar no tutorial algumas destas ferramentas, de acordo com o tempo de apresentação, sendo que o autor possui experiência na maioria delas.

IV. ESTUDOS DE CASO

A ideia é apresentar no tutorial dois estudos de caso reais, adaptados para que não sejam identificados os envolvidos. O primeiro estudo de caso se refere a uma análise *post-mortem* e o segundo a uma análise *live forensics*.

Na análise *post-mortem* será mostrado um caso de uma suposta vítima de engenharia social, a qual teria sua máquina infectada por algum *malware* e de alguma forma seus dados bancários teriam sido roubados. A vítima relata que após a análise de um extrato bancário de sua conta, achou estranho uma transferência financeira para uma conta que não conhecia. Como a vítima informou a data em que percebeu a transferência bancária. A vítima reclamou ao banco e este concordou em ressarci-la desde que fosse comprovada a fraude mediante perícia. Então foi registrado boletim de ocorrência e a própria vítima entregou seu computador.

Após ter recebido o equipamento para perícia, fotografias foram registradas, tanto externas quanto internas, foi verificado se havia alguma mídia de armazenamentos nos drives (disquetes, mídias ópticas), após o disco rígido foi retirado para a realização de duplicação forense (cópia bit-a-bit). Para a cópia foi utilizado a ferramenta Encase, garantindo a integridade do disco questionado.

A suspeita inicial seria alguma mensagem contendo engenharia social, então as caixas de e-mail foram analisadas partindo da data do incidente para trás. Foi verificado que uma semana antes, havia uma mensagem suspeita, solicitando que o usuário clicasse em um *link* para visualizar informações. O *link* em questão estava direcionando para um arquivo executável em um servidor fora do país. O *link* foi verificado e não estava mais ativo. Foi realizada uma busca pelo nome do arquivo e verificado que este se encontrava na imagem (cópia bit-a-bit) em análise. Tratava-se de um arquivo contendo o *keylogger* BPK, configurado para capturar todas teclas e cliques de mouse pressionados a partir da entrada em *sites* de seis bancos pré-definidos. Após, os dados seriam enviados para um servidor FTP no exterior, com usuário "teste" e senha "brasil" (configurações encontradas no *keylogger*).

Foram realizadas buscas por expressões regulares contendo o número da conta e outros dados relacionados à conta bancária da vítima. Nada foi encontrado. Após foram realizadas buscas nos diretórios onde seriam armazenadas as informações capturadas pelo *keylogger*. Nada foi encontrado relacionado à conta da vítima. Por fim foram realizadas buscas pelas palavras-chave "servidor FTP que estava configurado", "nome do usuário configurado", "senha configurada" e foram encontrados, na memória virtual (Windows), registros de acessos ao servidor FTP, usuário e senha configurados no *keylogger*, sendo possível verificar datas e horas de acesso, sendo estas posteriores ao recebimento do e-mail. Portanto, foram constatados que:

- havia uma mensagem de e-mail contendo engenharia social;
- a máquina estava infectada com um *keylogger* e o nome do arquivo infectado era o mesmo do *link* que estava no e-mail;
- havia indícios de acessos a um servidor FTP fora do país, com as mesmas configurações do *keylogger* e com datas posteriores ao recebimento do e-mail e infecção da máquina.

Logo tudo indica que houve a infecção da máquina e a vítima teve seus dados roubados através de um *malware*.

Na análise *live forensics* será mostrado um caso que a máquina estava ligada e foi possível realizar a cópia da memória RAM para posterior análise em laboratório. Após, foi solicitado à perícia todos diálogos (MSN Messenger ou outros) e senhas de qualquer tipo de serviço. Como no primeiro caso já foi abordada a análise *post-mortem*, neste segundo será abordada apenas a análise da memória RAM, não sendo abordada a análise do disco rígido.

A coleta dos dados (memória RAM) foi realizada com a distribuição Helix em um CD-ROM. A ferramenta utilizada foi a “dd” para Windows. A cópia foi gravada em um *pendrive* colocado no equipamento. Além da cópia *raw* (cópia bit-a-bit), foram gravados o *hash* e o *log* do que foi realizado.

Para a análise em laboratório foi utilizado o Encase, buscando palavras-chave como “msn”, “passwd”, password”, entre outras. Foram localizadas na imagem de memória RAM diversos trechos de diálogos do MSN Messenger, além de senhas digitadas em *sites*.

O passo a passo do que foi descrito e suas respectivas telas serão mostradas na apresentação deste tutorial.

V. CONSIDERAÇÕES FINAIS

Com a migração dos crimes do mundo "real" para o "digital" novas habilidades começaram a ser exigidas para a investigação. Muitos profissionais pensam que uma investigação ou uma perícia digital pode ser realizada por qualquer um que tenha conhecimento de informática.

Este tutorial mostrou que existem metodologias, boas práticas a serem seguidas, além da legislação brasileira, para evitar possíveis anulações de laudos em cortes da justiça, em casos em que o investigador ou perito não se preocupa em manter a integridade dos dados. Também foram mostradas ferramentas (hardware e software) para a realização de investigações ou perícias, desde as que não possuem custo até aquelas que possuem um alto custo.

Com todo o conteúdo apresentado, o aluno terá condições de ao menos saber por onde começar um trabalho relacionado à investigação digital ou onde pode atuar.

REFERÊNCIAS

[1] BRASIL. Código de Processo Penal. Decreto-Lei nº 3.689, de 3 de outubro de 1941, atualizado e acompanhado de legislação complementar, súmulas e índices. 10. ed. São Paulo: Saraiva, 2004.

[2] KENT, K.; CHEVALIER, S.; GRANCE, T.; DANG, H. Guide to Integrating Forensic Techniques into Incident Response: recommendations of the national institute of standards and technology. Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>. Acesso em: 15 abr. 2010.

[3] PEREIRA, E.; FAGUNDES, L.; NEUKAMP, P.; LUDWIG, G.; KONRATH, M. Forense Computacional: fundamentos, tecnologias e desafios atuais. In: VII SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, Rio de Janeiro. Minicursos ... Rio de Janeiro: VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2007.

[4] SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. Best Practices for Computer Forensics. Disponível em: <http://68.156.151.124/documents/swgde2006/Best_Practices_for_Computer_Forensics%20July06.pdf>. Acesso em: 15 abr. 2010.

[5] SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE. **SWGDE History**. Disponível em:<http://68.156.151.124/SWGDE_History.pdf>. Acesso em: 15 abr. 2010.

[6] Carrier, B. D. (2006). Risks of live digital forensic analysis. Commun. ACM, 49(2):56–61.

[7] Adelstein, F. (2006). Live forensics: diagnosing your system without killing it first. Commun. ACM, 49(2):63–66.

[8] Encase. Página oficial da ferramenta Encase. Disponível em:< http://www.guidancesoftware.com/computer-forensics-ediscovery-software-digital-evidence.htm>. Acesso em: 15 abr. 2010.

[9] FTK. Página oficial da ferramenta FTK. Disponível em:< http://www.accessdata.com/forensictoolkit.html>. Acesso em: 15 abr. 2010.

[10] E-fense: Helix. Disponível em: <http://www.e-fense.com/h3-enterprise.php>. Acesso em: 15 abr. 2010.

[11] FDTK-UbuntuBR. Disponível em: <http://www.fdtk.com.br>. Acesso em: 15 abr. 2010.

[12] PeriBR. Disponível em: <http://sourceforge.net/projects/peribr/>. Acesso em: 15 abr. 2010.

[13] Windows Sysinternals. Disponível em:<http://technet.microsoft.com/pt-br/sysinternals/default.aspx>. Acesso em: 15 abr. 2010.

[14] TABLEAU. Disponível em: <http://www.tableau.com/>. Acesso em: 15 abr. 2010.

Evandro Della Vecchia Pereira

Mestre em Ciência da Computação pela Universidade Federal do Rio Grande do Sul - UFRGS. Bacharel em Ciência da Computação pela Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Especialista em Perícias de Crimes de Informática – Associação Brasileira de riminalística. Perito Criminal (área Computação Científica) no Instituto Geral de Perícias – Secretaria de Segurança Pública do Estado do Rio Grande do Sul.

Perito relator de mais de cem laudos periciais de informática. Professor de ensino superior na Universidade do Vale do Rio dos Sinos (UNISINOS) e na Faculdade de Tecnologia SENAC (FATEC/SENACRS).

Leciona em cursos de Formação da Polícia Civil, Polícia Militar e Servidores do Instituto-Geral de Perícias, além de lecionar Cursos de Crimes Cibernéticos na Academia de Polícia do Estado do Rio Grande do Sul.

Possui publicações na área de redes de computadores e segurança da informação, incluindo um minicurso no Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2007) intitulado "Forense Computacional: fundamentos, tecnologias e desafios atuais". Link para o Currículo Lattes: http://lattes.cnpq.br/2539523750445675