Forense Computacional: Aspectos Legais e Padronização

Célio Cardoso Guimarães
Instituto de Computação - UNICAMP
CP 6176 - 13083-970 Campinas - SP
celio@ic.unicamp.br

Flávio de Souza Oliveira[1]
Instituto de Computação - UNICAMP
13083-970 Campinas - SP
flavio.oliveira@ic.unicamp.br

Marcelo Abdalla dos Reis[2]
Instituto de Computação - UNICAMP
13083-970 Campinas - SP
marcelo.reis@ic.unicamp.br

Paulo Lício de Geus
Instituto de Computação - UNICAMP
CP 6176 - 13083-970 Campinas - SP
paulo@ic.unicamp.br

Resumo

Com o advento da computação e o surgimento da Internet tornaram-se possíveis vários tipos de crimes eletrônicos, o que vem obrigando as agências legais a se prepararem para investigar casos que envolvam a computação. Contudo, em grande parte dos casos, os delitos são transjuridicionais, aumentando assim, a necessidade de intercâmbio e impulsionando a padronização no tratamento de evidências digitais.

1. Introdução

A forense computacional é um campo de pesquisa relativamente novo no mundo e está desenvolvendo-se principalmente pela necessidade das instituições legais atuarem no combate aos crimes eletrônicos. No Brasil conta-se ainda com poucos pesquisadores na área e existem poucas normas estabelecidas, o que gera um grande número de possibilidades de pesquisa.

A eliminação de fronteiras oferecida pela Internet gerou um grande problema para as instituições de combate ao crime, uma vez que facilitou em muito a ocorrência de crimes eletrônicos onde a vítima e o criminoso encontram-se em países distintos. Criou-se assim a obrigatoriedade de troca de informações e evidências eletrônicas entre as agências, contudo, por se tratar de uma necessidade muito recente, ainda não se conta com padrões internacionais para o tratamento desse tipo de evidência, dessa forma o valor jurídico de uma prova eletrônica manipulada sem padrões devidamente pré-estabelecidos poderia ser contestável.

Este trabalho é um *survey* que aborda basicamente o problema da padronização da análise forense computacional, bem como algumas implicações legais ligadas à sua prática. O objetivo é fornecer ao leitor um pano-

1. Financiado pela BOSCH
2. Financiado pela FAPESP

rama do atual estágio do debate, e apresentar as principais entidades ligadas ao assunto. Existe contudo a preocupação de apresentar a ciência forense para aqueles que não estão familiarizados com ela, como se pode constatar na seção 2.

2. Forense Computacional

A Forense Computacional foi criada com o objetivo de suprir as necessidades das instituições legais no que se refere à manipulação das novas formas de evidências eletrônicas. Ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional [3].

> *"Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system."* Dan Farmer e Wietse Venema [2]

Ao contrário das outras disciplinas forenses, que produzem resultados interpretativos, a forense computacional pode produzir informações diretas, que por sua vez, podem ser decisivas em um dado caso [3]. Isso pode ser notado no exemplo muito simples que se segue: no caso de um assassinato, o legista verifica que há traços de pele em baixo das unhas da vítima, isso é interpretado como um indício de que houve luta antes da consumação do crime, contudo não passa de uma interpretação. Já no caso de uma perícia em uma máquina suspeita podem ser conseguidos arquivos incriminadores como diários e agendas.

O problema de resolver um mistério computacional nem sempre é fácil, existe a necessidade de não se observar o sistema como um usuário comum e sim como um detetive que examina a cena de um crime [2]. Felizmente os programadores levam alguma vantagem neste assunto, pois muitas das habilidades necessárias para se procurar um erro em um código fonte, são também necessárias para uma análise forense, tais como: raciocínio lógico, entendimento das relações de causa e efeito em sistemas computacionais e talvez a mais importante, ter uma mente aberta.[2]

Uma perícia em um computador suspeito de invasão ou mesmo um computador apreendido em alguma batida policial envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise. Existe a necessidade de se conhecer minúcias do sistema operacional para que se tenha uma noção global de todos os efeitos das ações do perito [7]. Quanto à necessidade de se utilizar ferramentas específicas para análise, esta decorre da obrigatoriedade de não se perturbar o sistema que está sendo analisado, perturbações essas que podem ser traduzidas como mudanças nos tempos de acesso aos arquivos (*MAC times*) por exemplo, anulando assim uma das mais poderosas formas de se reconstituir o que aconteceu na máquina em um passado próximo. Ferramentas convencionais não têm a preocupação de manter a integridade dos tempos de acesso.

2.1 Privacidade

Ao se fazer uma análise forense em uma máquina, sobretudo se ela atua como servidor de serviços, tais como e-mail ou arquivos, deve-se tomar uma série de cuidados a fim de se evitar a invasão da privacidade dos usuários do

sistema. Apesar de serem raras as vezes em que se deve fazer uma busca em todos os arquivos de uma máquina, seja pela natureza do que se está procurando ou por limitações de processamento, já que um grande servidor pode conter uma capacidade de armazenamento muito grande, o que tornaria proibitiva tal operação. O ideal é que se defina um escopo, restringindo ao máximo a área de atuação da análise, evitando-se violar a privacidade de inocentes.

O problema da violação de privacidade muitas vezes pode ser contornado através da instituição de uma política de segurança clara e de conhecimento de todos os usuários, que contemple a possibilidade de vistoria em arquivos, e-mails e outros dados pessoais. Tal possibilidade deve ser seguida pela identificação de quem teria o poder para vasculhar os arquivos alheios, das circunstâncias em que essa medida pode ser tomada e de como o dono dos arquivos será notificado.

Políticas de segurança que contêm tais abordagens são bastante discutidas assim como a instalação de câmeras na sala do café, ou mesmo na sala onde se concentram os servidores; tais medidas poderiam causar polêmica em qualquer empresa. Contudo, deve-se conseguir um consenso na definição dos eventos que podem gerar a "quebra do sigilo eletrônico", de forma que esta deve-se tratar de uma medida extrema.

2.2 Implicações Legais

As evidências resultantes da análise forense podem afetar inúmeras investigações dramaticamente, nenhuma nova disciplina forense teve tanto potencial desde o DNA [3].

No Brasil não existem normas específicas que regem a forense computacional, contudo existem normas gerais que abrangem todos os tipos de perícia (ditadas no Código de Processo Penal), podendo ser adotadas no âmbito computacional, salvo algumas peculiaridades. No caso de uma perícia criminal existe a figura do Perito Oficial (dois para cada exame), onde o seu trabalho deve servir para todas as partes interessadas (Polícia, Justiça, Ministério Público, Advogados, etc.). Para se fazer perícia criminal, o profissional precisa ter nível universitário e prestar concurso público específico, podendo existir porém a figura do perito "ad hoc" para o caso de não existirem peritos oficiais disponíveis [1]. Logo quando se descobre uma invasão na rede deve-se imediatamente entrar em contato com as organizações de resposta a incidentes de segurança e tomar todas as medidas legais cabíveis.

A responsabilidade do perito no exercício da sua função deve ser dividida em duas partes distintas: aquela do ponto de vista legal, onde lhe são exigidas algumas formalidades e parâmetros para a sua atuação como perito; e as de ordem técnica, necessárias para desenvolver satisfatoriamente os exames técnico-científicos que lhe são inerentes [1].

O perito deve seguir à risca as normas contidas no Código de Processo Penal, dentre elas pode-se destacar duas para exemplificar a sua possível abordagem computacional:

- Art. 170. *Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.*

É sempre possível fazer cópias assinadas digitalmente das mídias que estão sendo investigadas para que possam ser feitas análises futuras se necessário. Na verdade o interessante é sempre atuar em cima de cópias, como será visto na sessão seguinte.

- Art. 171. *Nos crimes cometidos com destruição ou rompimento de obstáculo a substração da coisa, ou por meio de escalada, os peritos, além de descrever os vestígios, indicarão com que instrumentos, por que meios e em que época presumem ter sido o fato praticado.*

Existe a necessidade de se documentar quais as ferramentas de software utilizadas para se fazer a análise, bem como a possível identificação de uma linha de tempo, que pode vir a ser conseguida através da análise dos *MAC times*.

Paralelos assim podem ser feitos a fim de se garantir o valor judicial de uma prova eletrônica enquanto não se tem uma padronização das metodologias de análise forense.

3. Padronização na Aquisição de Evidências

Um antigo problema encontrado pelas instituições legais norte americanas, era a identificação de recursos dentro da organização que poderiam ser usados para se examinar uma evidência computacional, uma vez que esses recursos estavam espalhados através das agências. Atualmente parece existir uma tendência à mudança desses exames para o ambiente laboratorial. Em 1995, uma pesquisa conduzida pelo serviço secreto norte americano indicou que 48% das agências tinham laboratórios de forense computacional e que 68% das evidências encontradas foram encaminhadas a peritos nesses laboratórios e, segundo o mesmo documento, 70% dessas mesmas agências fizeram seu trabalho sem um manual de procedimentos [4].

Políticas devem ser estabelecidas para a manipulação de uma evidência computacional e, a partir dessas políticas, desenvolver protocolos e procedimentos. Tais políticas devem refletir os objetivos de toda comunidade científica, provendo resultados válidos e reproduzíveis. Contudo, a forense computacional é diferente das outras disciplinas forenses, uma vez que não se pode aplicar exatamente o mesmo método a cada caso [3]. Tome como exemplo a análise feita no DNA recolhido de uma amostra de sangue na cena de um crime, pode-se aplicar exatamente o mesmo protocolo a toda amostra de DNA recebida (elimina-se as impurezas e o reduz à sua forma elementar). Quando se tratam de ambientes computacionais não se pode executar o mesmo procedimento em todos os casos, uma vez que se têm sistemas operacionais diferentes, diferentes mídias e diversas aplicações.[3]

3.1 Principais Entidades

- IOCE (*International Organization on Computer Evidence*): Principal entidade internacional centralizadora dos esforços de padronização. Ela foi estabelecida em 1995 com o objetivo de facilitar a troca de informações entre as diversas agências internacionais, sobre a investigação de crimes envolvendo computadores ou outros assuntos forenses relacionados ao meio eletrônico. A IOCE identifica e discute assuntos de interesse dos seus constituintes, facilitando assim a disseminação da informação e desenvolvendo recomendações para os membros da organização. Além de formular padrões para evidências computacionais, a IOCE desenvolve serviços de comunicação entre as agências e organiza conferências.

- SWGDE (*Scientific Working Group on Digital Evidence*): Criado em 1998, ele é o representante norte americano nos esforços de padronização conduzidos pela IOCE.
- HTCIA (*High Technology Crime Investigation Association*): Organização sem fins lucrativos que visa discutir e promover a troca de informações que possam auxiliar no combate ao crime eletrônico.[9]
- IACIS (*International Association of Computer Investigatibe Specialists*): Trata-se de uma associação sem fins lucrativos, composta por voluntários, com o intuito de atuar no treinamento em forense computacional.
- SACC (Seção de Apuração de Crimes por Computador): Atua no âmbito do Instituto Nacional de Criminalística/Polícia Federal, a fim de dar suporte técnico às investigações conduzidas em circunstâncias onde a presença de materiais de informática é constatada.

3.2 Padronização Internacional

Com o advento da Internet e da consolidação do mundo globalizado, tornaram-se comuns as notícias de crimes transjuridicionais, obrigando as agências legais de vários países definirem métodos comuns para o tratamento de evidências eletrônicas. Evidentemente cada nação conta com sua legislação e não seria possível a definição de normas gerais para todos. A padronização aqui citada refere-se à troca de evidências entre países.

Atualmente já existem padrões definidos e sendo aplicados de forma experimental. Eles foram desenvolvidos pelo SWGDE e apresentados na *International Hi-Tech Crime and Forensics Conference* (IHCFC), que foi realizada em Londres, de 4 a 7 de outubro de 1999. Os padrões desenvolvidos pelo SWGDE seguem um único princípio, o de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiança e a exatidão das evidências. Esse nível de qualidade pode ser atingido através da elaboração de SOPs (*Standard Operating Procedures*), que devem conter os procedimentos para todo tipo de análise conhecida, e prever a utilização técnicas, equipamentos e materiais largamente aceitáveis na comunidade científica [5].

3.3 No Brasil

Ainda não existe padronização em andamento, apenas trabalhos feitos a pedido da polícia federal, trabalhos esses direcionados ao público leigo composto por promotores e juizes federais. As análises forenses são realizadas por instituições externas à polícia federal.

Seguem abaixo algumas instituições que possivelmente estariam envolvidas em um esforço de padronização nacional:

- NBSO (*Network Information Center (NIC) - Brazilian Security Office*): atua coordenando as ações e provendo informações para os sites envolvidos em incidentes de segurança. [10]
- CAIS(Centro de Atendimento a Incidentes de Segurança): tem por missão o registro e acompanhamento de problemas de segurança no backbone e PoPs da RNP, incluindo auxílio à identificação de invasões e reparo de danos causados por invasores. Cabe, ainda, ao CAIS a disseminação de informações sobre ações preventivas relativas a segurança de redes.[11]
- GT-S: grupo de trabalho em segurança do comitê gestor da internet brasileira.[11]

4. Conclusão

A padronização internacional ainda está distante de ser alcançada devido ao gargalo legal envolvido, visto que cada país conta com sua legislação específica. Além das dificuldades técnicas em se conceber padrões flexíveis que se adaptem às rápidas mudanças tecnológicas. Em se falando de Brasil, fica clara a atual desorganização; o Brasil não deve ficar alheio às discussões internacionais, para que não se corra o risco de haver incompatibilidades futuras entre a legislação internacional e os interesses nacionais.

5. Glossário [1]

- criminalística: ciência que se utiliza do conhecimento de outras ciências para poder realizar o seu mister, qual seja, o de extrair informações de qualquer vestígio encontrado em local de infração penal, que propiciem a obtenção de conclusões acerca deste fato ocorrido, reconstituindo os gestos do agente da infração e, se possível, identificando-o.
- perícia cível: trata dos conflitos judiciais na área patrimonial e/ou pecuniário.
- perícia criminal: é aquela que trata das infrações penais, onde o Estado assume a defesa do cidadão em nome da sociedade.
- perito: denominação dada aquele profissional que realiza os exames necessários para viabilizar a criminalística, qual seja, todos os exames que envolvem o universo possível em cada situação, para chegar a chamada materialidade do delito, também chamado de prova material ou científica.
- perícia: conjunto de exames realizados no universo da criminalística.

6. Referências

[1] ESPINDULA, Alberi; *A Função Pericial do Estado*; Perícia Criminal - DF; http://www.apcf.org.br;

[2] FARMER, Dan; VENEMA, Wietse; *Forensic Computer Analysis: An Introduction*; Dr. Dobb's Journal; setembro 200;

[3] NOBLETT, Michael G.; POLLITT, Mark M.; PRESLEY, Lawrence A.; *Recovering and Examining Computer Forensic Evidence*; Forense Science Communications, outubro 2000, Vol. 2 N. 4; Federal Bureau of Investigation;

[4] NOBLETT, Michael G.; *Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence*; Proceedings of the 11th INTERPOL Forensic Sciense Symposium; 1995

[5] SWGDE, Scientific Working Group on Digital Evidence; IOCE, International Organization on Digital Evidence; *Digital Evidence: Standards and Priciples*; Forense Science Communications, abril 2000, Vol. 2 N. 2; Federal Bureau of Investigation;

[6] SWGMAT, Scientific Working Group on Materials Analysis; *Trace Evidence Recovery Guidelines*; Forense Science Communications, outubro 1999, Vol. 1 N. 3; Federal Bureau of Investigation;

[7] http://www.porcupine.org; Website do Dr. Wietse Venema;

[8] http://www.fbi.gov

[9] http://www.htcia.org

[10] http://www. nic.br/nbso.html

[11] http://www.cais.rnp.br