Aplicação de *Live Forensics* para Captura de Senhas e Outros Dados Sensíveis

Evandro Della Vecchia
Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS
Instituto-Geral de Perícias/RS – Seção de Informática Forense

***Resumo* — A Perícia Digital surgiu da necessidade de investigação de crimes cometidos com a utilização de computadores e similares. Há basicamente duas formas de coletar os dados para análise: com o computador desligado (*post mortem forensics*) ou com o computador ligado (*live forensics*). A principal vantagem de realizar a coleta com o computador ligado é a possibilidade de se conseguir dados que se encontram apenas na memória RAM e que não são armazenadas em disco (ou são armazenadas de forma protegida, através de criptografia, esteganografia ou outra técnica). O objetivo deste trabalho é mostrar os conceitos, alguns softwares e experimentos para a coleta e análise de dados da memória RAM.**

***Palavras-chave* — perícia digital, forense digital, crime cibernético, crime digital, *live forensics*, análise da memória RAM.**

I. INTRODUÇÃO

Atualmente é comum ver notícias relacionadas a crimes cibernéticos a todo momento. Na verdade, muitos criminosos simplesmente migraram de práticas manuais para eletrônicas. Ou seja, quem falsificava documentos sem um computador começou a utilizá-lo, para facilitar suas atividades.

Para constituir a prova técnica existe a perícia criminal, pois é necessário que alguém especializado em determinado assunto possa traduzir o que foi encontrado para um formato (Laudo Pericial) que seja compreensível a juízes, delegados e outros profissionais.

Porém, muitos indivíduos começaram a se preocupar em esconder ou destruir dados, dificultando a análise pericial. Nestes casos, a simples apreensão de equipamentos para futura análise pode não ser eficaz. Um exemplo é o uso de criptografia, sendo necessário descobrir a senha utilizada para gerar uma chave de decriptação do conteúdo protegido. Esta senha geralmente não fica armazenada e pessoas bem instruídas não a anotam em papéis ou em outros locais.

Para casos em que há proteção e há a possibilidade do flagrante (computador ligado), é possível coletar dados de documentos e programas que estão na memória RAM, inclusive dos que já foram fechados.

II. CONCEITOS DE PERÍCIA DIGITAL

A Perícia Digital faz parte de um processo investigativo, que tem como objetivo a apuração dos fatos ocorridos com a maior clareza possível. Pode ser realizado por um perito criminal (concursado), perito nomeado ou por um profissional contratado para realizar o trabalho em uma empresa. Independente da esfera em que o perito for atuar (criminal, cível ou particular) é importante que este trabalhe de uma forma sistemática e cuidadosa com as evidências com a intenção de sempre preservar a integridade dos dados e detalhar toda a atividade executada nos resultados (Laudo Pericial).

Ao iniciar o procedimento de perícia em um equipamento questionado, o perito deve fazer a escolha de qual metodologia será empregada em seu trabalho: a *Live Forensics*, a *Post Mortem Forensics*, ou ambas [1][2].

A metodologia ***Live Forensics*** (foco deste trabalho) 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 em execução no computador, conexões de rede estabelecidas, dados da memória principal (RAM), 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* ou outros *malwares* 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 por boas práticas a criação de uma cópia *bit a bit* (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 algoritmos de *hash*.

A escolha da metodologia adequada vai depender do tipo de delito que será investigado. Por exemplo, em um suposto crime de estelionato, 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.

Uma situação que exige a aplicação de *Live Forensics* é quando há a suspeita de utilização de técnicas de proteção dos dados no disco, como por exemplo, a criptografia e a esteganografia. Ou ainda, a utilização de softwares configurados para não registrar *logs*, como por exemplo, o uso do MSN Messenger configurado para não gravar os diálogos. Nestes casos, é possível recuperar alguns diálogos e/ou senhas utilizadas.

De acordo com boas práticas o procedimento pericial é divido em etapas. Conforme descrito em [3] e [4], quatro etapas podem descrever todo o procedimento (Figura 1).

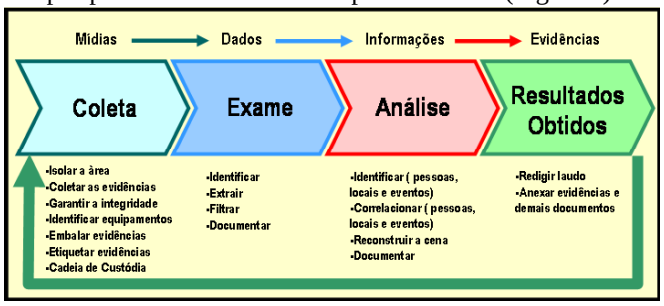

Figura 1: Etapas do processo de perícia digital [4].

Abaixo as quatro etapas são explicadas, com ênfase na metodologia *Live Forensics*.

Coleta de dados

Esta etapa é de extrema importância, pois se for mal realizada pode implicar na invalidação da prova. É nela que toda a massa crítica de dados será coletada, sendo necessário cuidado especial para manter a integridade dos dados [5].

Obviamente não é possível garantir que nada na memória RAM seja alterado, pois o simples fato de executar uma aplicação para realizar a coleta de dados já altera seu estado. O importante é que a aplicação escolhida altere o mínimo possível da memória, ou seja, os processos criados pela execução de softwares deve ocupar pouco espaço.

A RFC 3227 [6] elenca a seguinte ordem de volatilidade: (1) registradores, cache; (2) tabela de roteamento, cache ARP, tabela de processos, estatísticas do *kernel*; (3) memória; (4) arquivos temporários; (5) disco; (6) registros (*logs*) remotos que sejam relevantes ao sistema em questão; (7) configuração física, topologia da rede; (8) mídias de arquivamento. Para a captura de dados com a máquina ligada, os itens 1, 2 e 3 merecem maior importância.

Outras atividades realizadas nesta etapa são relacionadas ao equipamento questionado, que deve ser identificado, fotografado, devidamente embalado de uma forma segura, e tudo deve ser registrado em um documento, denominado 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, é possível 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.

No caso de *Live Forensics*, a busca por palavras-chave é o procedimento mais utilizado, pois é possível procurar trechos de e-mails, conteúdo de sítios navegados, trechos de texto digitados pelo usuário, senhas digitadas, entre outros.

Análise das Informações

Na terceira etapa, as informações anteriormente separadas serão analisadas com o intuito de encontrar dados 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]. Muitas vezes a análise resulta em novas palavras-chave que devem ser pesquisadas na etapa de exame dos dados.

Resultados

Nesta última etapa, o objetivo é apresentar um Laudo Pericial (relatório técnico) que deve informar com veracidade e objetividade o que foi encontrado nos dados analisados. Todo o processo pericial, as ferramentas utilizadas e informações que comprovem a integridade das informações devem ser relatadas no Laudo [5].

III. SOFTWARES E EXPERIMENTOS

Nesta seção serão mostrados softwares que permitem a coleta e exame de dados, pois a análise é feita pelo perito e para os resultados o perito utiliza um editor de texto e softwares para gravação de mídias (CDs/DVDs) quando necessário para o anexo.

Serão mostrados softwares para o ambiente Windows, por ser o sistema mais utilizado em equipamentos analisados pela perícia, de acordo com a experiência do autor.

Antes de realizar o *dump* de memória (coleta integral da memória RAM), é interessante coletar dados que sejam mais fácil visualizar. O fabricante Nirsoft [7] possui diversos softwares para este fim. Abaixo serão mostrados apenas três deles.

LastActivityView

O nome sugere a visualização das últimas atividades, mas no exemplo mostrado na Figura 2 são mostradas atividades desde 2006 até o momento do teste (27/09/2013).

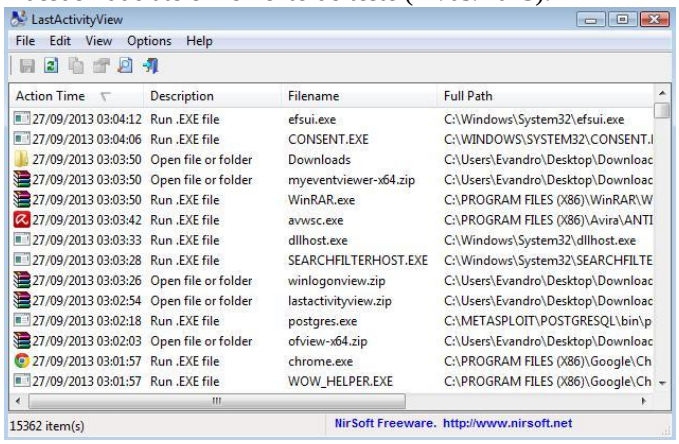

Figura 2: Atividades realizadas.

WinLogOnView

Este software mostra informações de *logon*, tais como: usuário, data/hora de início e fim, domínio, endereço IP, entre outros. Um exemplo é mostrado na Figura 3

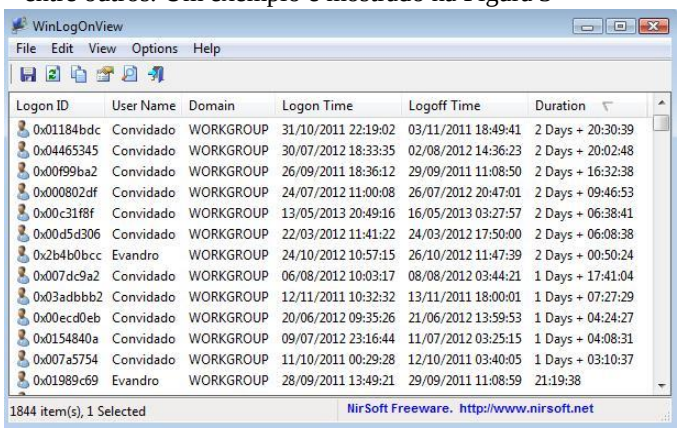

Figura 3: Informações de *logon*.

MyEventViewer

Mostra eventos de segurança do Windows. Um exemplo é mostrado na Figura 4.

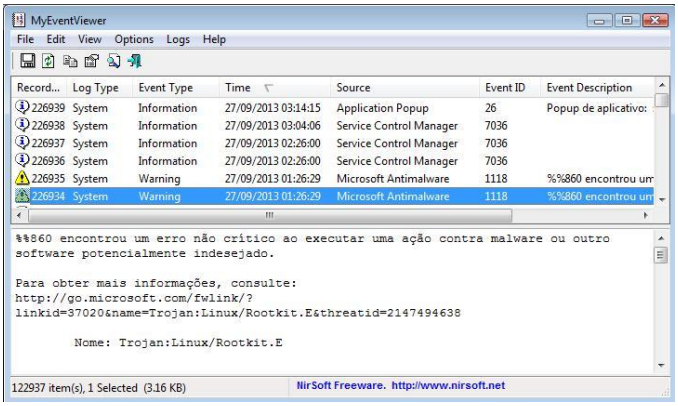

Figura 4: Visualização de eventos.

Para a realização de *dump* de memória, um software que funcionou e em um tempo considerado satisfatório (4GB em cerca de 2min20s) foi o Belka Live RAM Capturer [8]. Além de fácil utilização, não é necessário instalar e ocupa cerca de 2MB na memória. A Figura 5 mostra a coleta de 4GB de memória RAM, a qual será filtrada com palavras-chave posteriormente.

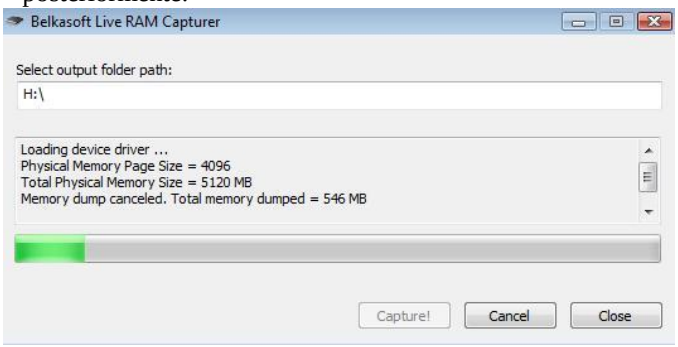

Figura 5: Coleta integral da memória RAM (*dump*).

Para a realização dos experimentos, antes da coleta algumas contas de e-mail foram acessadas e e-mails foram enviados, alguns sítios foram acessados e textos foram digitados. Após estas atividades, todas as janelas foram fechadas e o *dump* da memória realizado.

Um bom software para abrir o arquivo de *dump* de memória é o FTK Imager [9]. Através da operação *Find* (CTRL F) é possível procurar por palavras-chave. Por exemplo, se o perito quer procurar contas de e-mail Gmail, pode procurar por "@gmail.com". As Figuras 6 a 9 mostram alguns dados encontrados, que poderiam auxiliar em uma possível investigação.

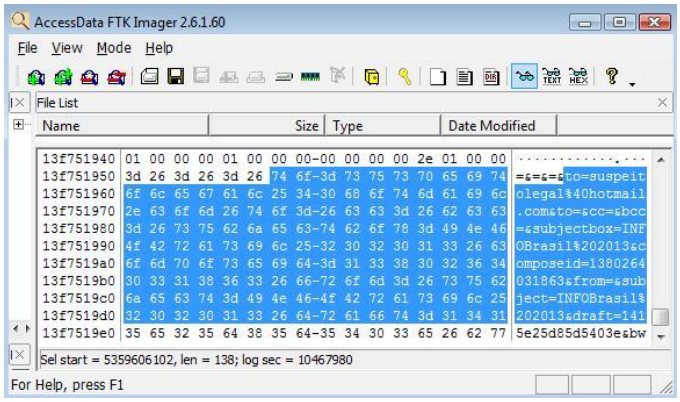

Figura 6: Alguns cabeçalhos de um e-mail.

Na Figura 6 é possível visualizar que um e-mail foi enviado para suspeitolegal@hotmail.com, com o assunto INFOBrasil 2013. Na Figura 7 é possível visualizar o conteúdo deste e-mail: "Este evento é muito bom e espero que a palestra sobre Live Forensics agrade a todos! Um grande abraço!".

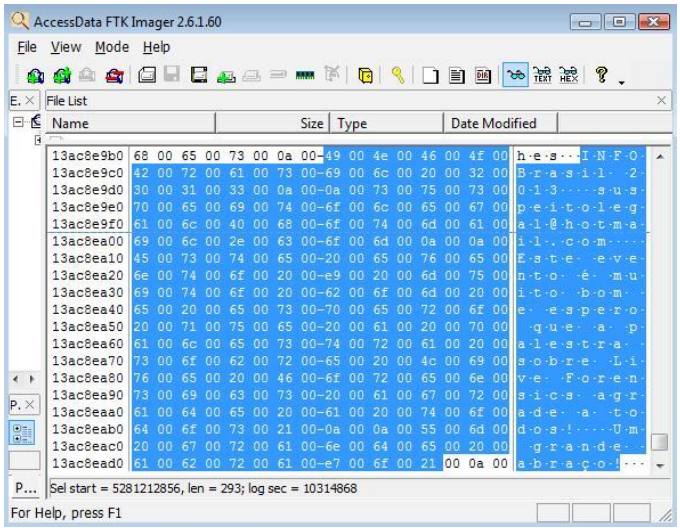

Figura 7: Conteúdo de um e-mail.

As Figuras 8 e 9 mostram senhas de contas de e-mail, sendo 123456teste a senha da conta testepericia@gmail.com e suspei654321 a senha da conta suspeitolegal@hotmail.com.

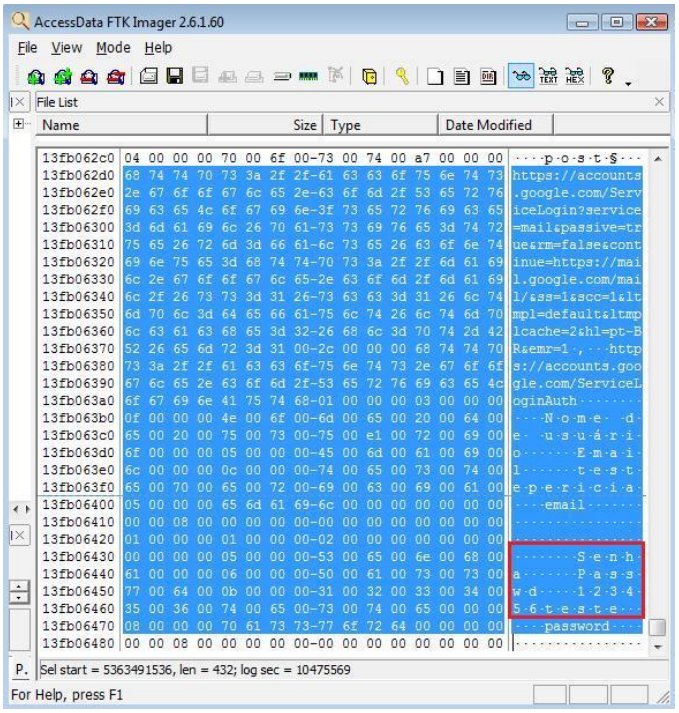

Figura 8: Senha de uma conta do Gmail.

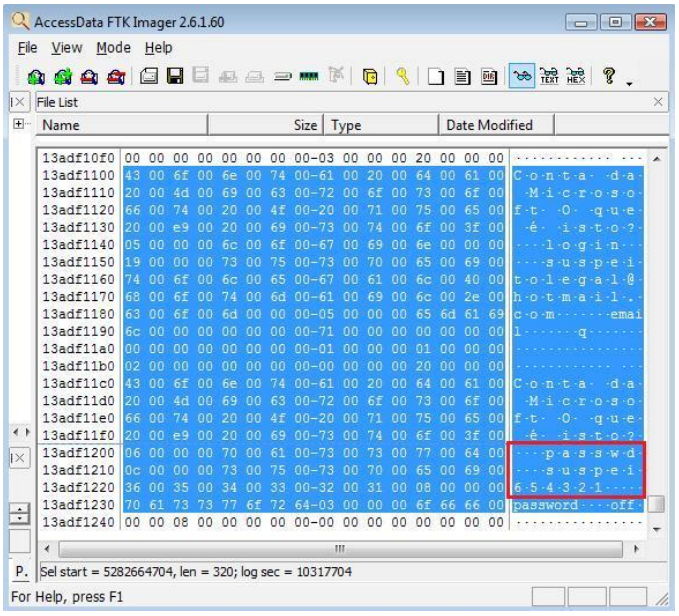

Figura 9: Senha de uma conta do Hotmail.

IV. CONSIDERAÇÕES FINAIS

Com a migração dos crimes do mundo real para o "mundo 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 trabalho mostrou que existem boas práticas e softwares adequados para a realização de perícias, com enfoque na coleta de dados da memória RAM (*Live Forensics*). Esta metodologia tem se tornado cada vez mais

importante, visto que muitas pessoas têm utilizado técnicas que dificultam ou impossibilitam a coleta de dados de mídias (discos, cartões de memória, etc.), como por exemplo: a não gravação de *logs*, o uso de criptografia, o uso de *Wipe*, entre outros.

REFERÊNCIAS

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

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

[3] 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". NIST, 2006.

[4] Della Vecchia, 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, Minicursos. Rio de Janeiro, 2007.

[5] Scientific Working Group on Digital Evidence "Best Practices for Computer Forensics". Disponível em: <https://www.swgde.org/documents/Current%20Documents/09-14-2013%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-0>. Acesso em: out. 2013.

[6] Brezinski, D.; Killalea, T. "Guidelines for Evidence Collection and Archiving", Request for Comments: 3227, IETF, 2002.

[7] Nirsoft – freeware utilities: password recovery, system utilities, desktop utilities. Disponível em <http://www.nirsoft.net/>. Acesso em: out. 2013.

[8] Belkasoft: Digital Evidence Extraction Software for Computer Forensic Investigations. Disponível em <http://forensic.belkasoft.com>. Acesso em: out. 2013.

[9] Computer Forensics Software for Digital Investigations. Disponível em <http://www.accessdata.com/products/digital-forensics/ftk>. Acesso em: out. 2013.

Evandro Della Vecchia

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 Criminalística. Perito Criminal (área Computação Científica) no Instituto Geral de Perícias – Secretaria de Segurança Pública do Estado do Rio Grande do Sul desde 2004.
Professor de ensino superior desde 2006, lecionando desde 2011 na PUCRS. Leciona em cursos de Formação da Polícia Civil (ACADEPOL), da Polícia Militar, de Servidores do Instituto-Geral de Perícias (IGP/RS), além de cursos de Pós-Graduação nas áreas de Perícia Digital, Auditoria de T.I. e Segurança da Informação em diversas universidades.
Possui publicações nas áreas 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" e um a ser publicado no SBSeg 2013, intitulado "Anti-Forense Digital: conceitos, técnicas, ferramentas e estudos de caso".
Link para o Currículo Lattes: http://lattes.cnpq.br/2539523750445675