Forense Computacional em Memória Principal

Antônio Pires de Castro Júnior é Mestre em Ciência da Computação pela Unicamp, Prof. Universitário e Técnico Judiciário do Poder Judiciário do Estado de Goiás. Bruno Lopes Lisita, Thiago Silva Machado de Moura e Tiago Jorge Pinto são Especialistas em Segurança em Redes de Computadores pela FATESG/SENAI

Resumo—**A perícia em sistemas computacionais é comumente praticada apenas em discos rígidos e outros dispositivos de armazenamento não volátil. Entretanto, evidências podem ser encontradas na memória principal de um computador, como programas e processos sendo executados, além de arquivos que não estão protegidos por senhas ou criptografia como nos discos rígidos. Pela característica da memória principal ser "volátil" torna-se um lugar desprezado pela maioria dos peritos, pois geralmente o computador já fora reiniciado ou mesmo desligado. Este trabalho acadêmico de final de curso de pós-graduação em Segurança da Informação, prova que, mesmo após a interrupção de energia, é possível encontrar vestígios de dados antigos contidos na memória RAM, seguindo os procedimentos corretos, como tempo, temperatura e programas específicos. Desta forma, podemos concluir no final deste trabalho em laboratório, que a memória principal (RAM) não é tão volátil e abre possibilidades de coleta de evidências em lugar desprezado pela maioria dos peritos em Forense Computacional.**

***Palavras-chave*—Forense Computacional, memória principal, perícia forense, segurança de computadores e coleta de evidências.**

I. INTRODUÇÃO

ATUALMENTE, os computadores estão cada vez mais presentes nas ações cotidianas, como comprar algum produto ou efetuar pagamentos de contas, e em questões mais pessoais, como um meio para conversar ou fazer anotações e registros da vida real.

Como em todas as áreas, existem pessoas que fazem uso dos sistemas computacionais para a prática de atos ilícitos. Com isso, torna-se necessário utilizar técnicas de ciência forense computacional para investigar crimes que foram cometidos utilizando equipamentos e sistemas computacionais, tanto para crimes digitais, como para crimes que não foram cometidos através deles.

A forense computacional tem a função de provar que um crime foi praticado através de recursos computacionais, de forma que os resultados obtidos na perícia técnica não gerem dúvidas quanto a sua integridade e não repúdio, bem como coletar evidências para ajudar em investigações e/ou processos judiciais.

A crescente onda de crimes cometidos através de computadores se dá, dentre muitos casos, pelo fato das pessoas ainda serem leigas no que diz respeito à segurança de sistemas computacionais e informações, além de pensarem que a Internet garante o anonimato, que se pode fazer qualquer coisa, e que não será punido no mundo real.

Objetiva-se, neste trabalho, provar que é possível coletar dados/evidências da memória principal (RAM) mesmo após a máquina ter sido desligada, provando que a memória principal não é tão volátil, permitindo encontrar dados dependendo do tempo e técnicas utilizadas. Tem-se a intenção, também, de verificar qual a relação da temperatura com a capacidade de manter a informação em memória principal.

II. FORENSE COMPUTACIONAL

A Forense Computacional é o ramo da criminalística que envolve a aquisição, preservação, restauração e análise de evidências computacionais, tanto em elementos físicos, como em dados que foram processados eletronicamente e armazenados em mídias computacionais.

O propósito de um exame forense é a extração de informações de qualquer vestígio relacionado com o caso investigado, permitindo a formulação de conclusões sobre a denúncia feita.

Existem duas abordagens no que diz respeito ao objetivo final da análise forense, uma é a análise buscando obter informações de valor probante, coerentes com as regras e leis sobre evidências, sendo admissíveis em uma corte de justiça, para serem utilizadas em um processo criminal. A outra abordagem é o exame realizado dentro de uma empresa com o objetivo de determinar a causa de um incidente e assegurar que as medidas disciplinares sejam aplicadas aos verdadeiros responsáveis [13].

A. Evidência Digital

Na ciência forense existe o chamado Princípio da Troca de Locard [13], o qual diz que qualquer um ou qualquer coisa que entra num local de um crime, leva consigo algo do local e deixa alguma coisa para trás quando vai embora. Na área computacional, este princípio também é válido, mas nem sempre se pode determinar que um pedaço de dado foi derivado de um crime ou retirar esses vestígios de modo a serem analisados de maneira eficaz, de acordo com as ferramentas atuais.

O termo evidência digital é atribuído a toda e qualquer informação digital capaz de determinar que uma intrusão aconteceu, ou que forneça alguma ligação entre o delito e as vítimas ou entre o delito e o atacante.

A evidência digital não deixa de ser um tipo de evidência física, embora seja menos tangível. Ela é composta de campos magnéticos, campos elétricos e pulsos eletrônicos que podem ser coletados e analisados através de técnicas e ferramentas

apropriadas. Entretanto, a evidência digital possui algumas características próprias [13]:

- Ela pode ser duplicada com exatidão, permitindo a preservação da evidência original durante a análise;
- Com os métodos apropriados, é relativamente fácil determinar se uma evidência digital foi modificada;
- A evidência digital é extremamente volátil, podendo ser facilmente alterada durante o processo de análise.

Toda informação relevante deve ser coletada em uma varredura meticulosa para análise, respeitando dois princípios básicos, o da autenticidade, onde se deve garantir a origem dos dados, e o da confiabilidade, que assegura que os dados são confiáveis e livres de erros. Conforme as evidências digitais são encontradas, elas devem ser extraídas, restauradas quando necessário (caso estejam danificadas ou cifradas), documentadas e devidamente preservadas. Em seguida, as evidências encontradas devem ser correlacionadas, permitindo a reconstrução dos eventos relacionados ao delito. Muitas vezes na análise das evidências, ao correlacionar e reconstruir os passos, promove-se a descoberta de novas informações, formando um ciclo no processo de análise forense.[13]

As principais fontes de informação de um sistema computacional são apresentadas a seguir, na ordem da maior volatilidade para a menor.

Dispositivos de Armazenagem da Unidade Central de Processamento (CPU)

As informações contidas nos registradores de uma CPU são de mínima utilidade e sua captura é impraticável. As *caches* podem conter informações que ainda não foram atualizadas na memória principal do sistema, mas estes dados não possuem nenhum valor de prova pericial por conter apenas cálculos em linguagem de máquinas impossíveis de serem traduzidos em informações com garantia.

Memória de Periféricos

Muitos dispositivos, como modems, placas de vídeo, aparelhos de fax e impressoras, contêm dados residentes nas suas memórias que podem ser acessados e salvos. Esses dados podem ser informações que não mais residem no sistema analisado, como gravações de voz, documentos e mensagens de texto ou números de telefone e fax.

Memória Principal do Sistema

A memória principal contém todo tipo de informação "volátil", como, por exemplo, informações de processos que estão em execução, dados que estão sendo manipulados e ainda não foram salvos no disco, e informações do sistema operacional, isto inclui informações em texto pleno que, em disco, estão cifradas. Os chamados *crash dump* contém uma imagem da memória do sistema no momento em que uma falha inesperada acontece (denominada de *crash*).

Tráfego de Rede

A partir de datagramas capturados, é possível reconstruir a comunicação entre o atacante e a máquina alvo, de modo que uma seqüência de eventos pode ser estabelecida e comparada com as outras evidências encontradas na máquina comprometida. Existem vários programas que podem ser usados para capturar o tráfego de rede, comumente denominados de *sniffers*, que além de capturar os datagramas que trafegam na rede, podem decodificá-los e exibi-los em um formato mais legível, ou, ainda, executar operações mais complexas como reconstrução de sessão e recuperação de arquivos transferidos pela rede [10].

Estado do Sistema Operacional

Informações relacionadas com o estado do sistema operacional podem fornecer pistas importantes quanto à existência, tipo e origem de um ataque em andamento. Tais informações representam uma imagem do sistema operacional em um determinado instante (processos em execução, conexões de rede estabelecidas, usuários logados, tabelas e *caches* mantidas pelo sistema) e geralmente são perdidas quando o sistema é desligado.[13]

Coletar informações acerca dos usuários logados no sistema, do estado das interfaces de rede e conteúdo das tabelas podem evidenciar um ataque ou alguma atividade incomum, como por exemplo, a existência de um possível *sniffer* no sistema, ou identificar uma alteração da tabela de rotas.

Módulos de Kernel

O núcleo do sistema (*kernel*) contém as funcionalidades básicas para o funcionamento do sistema operacional. Os núcleos anteriormente eram monolíticos, ou seja, para adicionar ou retirar uma funcionalidade era necessário compilação e instalação do novo *kernel*, além da necessidade de reiniciar o equipamento para o novo *kernel* entrar em uso. Para minimizar esse processo, pensou-se em permitir adicionar ou retirar recursos em tempo real, criando, então, os módulos de *kernel*. Esta vantagem também pode ser um problema para os sistemas operacionais, pois, uma vez invadido, o atacante pode carregar um módulo de *kernel* malicioso, com o propósito de esconder suas atividades das ferramentas de prevenção e auditoria do sistema, interceptar comandos do sistema e produzir resultados falsos.

Dispositivos de Armazenagem Secundária

O disco representa a maior fonte de informação para o exame forense computacional, e em cada porção dele, por menor que seja, onde se possa ler e/ou escrever um conjunto de bits, representa uma possível fonte de informação para a análise forense. Determinadas áreas do disco não são acessíveis através de um sistema de arquivos e podem conter informações que um atacante pode manter escondidas ou, ainda, vestígios que o mesmo tentou apagar. Com isso, podem ser classificadas as informações armazenadas em disco em duas classes: as acessíveis pelo sistema de arquivos (os arquivos propriamente ditos e seus atributos) e as informações armazenadas em áreas não acessíveis através do sistema de arquivos (espaços não alocados ou marcados como danificados, por exemplo).

Além disso, áreas do dispositivo de armazenagem podem conter informações "deletadas". Quando um arquivo é

apagado, sua referência é removida das estruturas do sistema de arquivos, entretanto, os dados contidos no arquivo não são apagados do disco. Tais dados permanecem no disco indefinidamente, até que sejam sobrescritos por outros arquivos. Sendo assim, arquivos completos ou porções menores podem ser recuperados após terem sido apagados e parcialmente sobrescritos.

Além de se obter informações sobre a configuração do disco, é importante efetuar a imagem *bit* a *bit* do dispositivo. Este tipo de imagem é diferente de uma cópia normal de arquivos, pois todo conteúdo do disco será copiado, incluindo os espaços não utilizados.[13]

B. *Fases de Uma Perícia Forense Computacional*

Algumas fases para realizar uma perícia forense computacional foram definidas no documento ***Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas*** em [13]. As fases são, basicamente:

- Considerações e Inteligências Preliminares;
- Planejamento;
- Coleta, Autenticação, Documentação e Preservação de Material Para Análise;
- Análise;
- Reconstrução dos Eventos

III. A Legislação Brasileira e o Perito em Forense Computacional

A legislação brasileira, disponente sobre crimes digitais, ainda trabalha por meio de jurisprudência, ou seja, não se tem uma lei específica ditando formas e tipos de crimes, e nem qual deve ser a punição. Os juízes julgam os criminosos correlacionando os delitos com artigos do Código Penal atual, como, por exemplo, crimes de roubo ou de injúria e difamação.

Assim, as penas dos crimes variam bastante em intensidade, pois muitos juízes não possuem auxílio de um bom profissional na área de informática ou mesmo de um perito computacional que possa revelar a ele os verdadeiros danos causados pelo criminoso. E, se utilizando da jurisprudência, muitos advogados recorrem nos processos apresentando outros casos em que a pena pelo mesmo tipo de crime foi mais branda, ou mesmo que o caso fora encerrado.

O perito em forense computacional segue a mesma legislação que peritos de outras áreas, assim como são definidas formas de como uma prova pericial se torna válida diante de um julgamento. E, para evitar punições previstas em lei ao perito, tem-se que tomar o máximo de cuidado para manusear o material periciado para que não contamine as evidências e, também, possibilitar que uma segunda perícia seja possível, caso solicitado.

Segundo a legislação, para ser um perito em um processo, a pessoa tem que ter curso superior específico na área técnica ou científica, com conhecimento técnico-formal, ser idônea e hábil. Estão impedidas de periciar as pessoas que não possuem capacidade para atos da vida civil, nem conhecimento técnico específico suficiente, pessoas que são: parte; testemunha; cônjuge ou qualquer outro parente, em linha reta ou colateral até o 3º grau, no processo (Código de Processo Civil, art. 134) e nos casos de suspeição, como: o amigo íntimo ou inimigo capital de uma das partes (CPC, art. 135).

Mais informações sobre as leis atuais e jurisprudências relacionadas à informática podem ser encontradas no documento ***Ferramentas para análise forense aplicada à Informática*** em [10].

Existe um novo projeto de lei em tramitação na Câmara dos Deputados Federal em Brasília, n° 89/03, de autoria do Senador Eduardo Azeredo, que visa estabelecer regras e punições para ações efetuadas através da computação, inclusive definindo delitos amplamente praticados na Internet.

O referido possibilitará atualizar a legislação brasileira para ser mais clara e específica nas questões de crimes relacionados a sistemas eletrônicos, digitais e similares, e praticados contra dispositivos de comunicação e sistemas informatizados e similares, além de rede de computadores. O projeto de lei especifica também deveres de fornecedores de serviços para que auxiliem nas investigações e identificação de criminosos que utilizaram dos serviços das mesmas para cometer infrações.

Com isso, será mais fácil para o perito identificar em qual crime uma infração é relacionada, e ações que antes não eram vistas como crimes propriamente ditos passarão a ser. Entretanto, este projeto deve ser devidamente analisado para se adequar à realidade brasileira, não criminalizando situações corriqueiras, além de prever todas as situações que a tecnologia mundial oferece às pessoas, para que a lei não caia em desuso ou não seja tão abrangente, de forma a tornar estático o desenvolvimento de idéias pelo fato de não se saber se está cometendo um crime ou não.

O profissional que atua na área de forense computacional pode ser chamado de perito ou investigador.

IV. Forense em Memória Principal

Grande parte dos trabalhos sobre forense computacional ainda se prende à análise de dados obtidos a partir do sistema de arquivos em dispositivos secundários. Essa escolha se explica por fatores como a maior facilidade para se isolar a "cena do crime" e a maior disponibilidade de ferramentas para este tipo de análise. Nesta situação o trabalho do perito, no ambiente alvo de perícia, se restringe inicialmente a garantir o isolamento lógico dos equipamentos, evitando ações internas ou externas que possam alterar ou eliminar evidências.

Partindo do pressuposto de que possa haver tentativas de alterar ou eliminar evidências usando comandos pela rede, ou mesmo "armadilhas" no próprio sistema, acionadas por determinadas ações, o mais seguro era simplesmente parar os sistemas, interrompendo diretamente o fornecimento elétrico ao equipamento, evitando processos normais de "*shutdown*", que também poderiam ter sido modificados para eliminar evidências em situações específicas. O próximo passo se resumia a recolher todos os dispositivos de armazenamento e gerar imagens para posterior análise.

Entretanto, é óbvio que ao ignorar os dados voláteis no processo de coleta de evidências, se perdem muitas informações importantes em um processo de análise forense, tais como: processos em execução, estados de conexões, portas TCP/UDP abertas, dados de programas em execução na memória, filas de conexões, conteúdos de *buffers*, senhas digitadas, chaves de arquivos criptografados que estavam em uso, entre outros. Alguns desses dados podem ser importantes até mesmo para possibilitar a análise de dados do sistema de arquivos.

A. A Memória Principal (RAM)

A memória RAM, sigla para *Random Access Memory* (Memória de Acesso Aleatório), é a responsável por armazenar informações para acesso rápido do processador.[6]

Como seu próprio nome já diz, a memória RAM tem como principal característica permitir o acesso direto a qualquer um dos endereços disponíveis, e é essa característica que a faz ser mais rápida do que, por exemplo, um HD (*Hard Disk*), diminuindo o tempo de resposta para o processador, já que trabalha com taxas de transferências de dados muito superiores.

Quando um programa é executado, ele é lido da mídia de armazenamento (HD, *Pen Drive*, etc...), e então transferido para a memória RAM. O processador busca todas as informações necessárias para a execução daquele programa diretamente da memória.

Este tipo de memória possui a desvantagem de que, por ser uma memória do tipo "volátil", quando a máquina é desligada, todos os dados contidos nela são perdidos.

O tipo mais usual de memória encontrada é a memória DRAM, *Dynamic RAM* (Memória de Acesso Aleatório Dinâmico). A memória DRAM começou a ser mais utilizada a partir do final da década de 70, substituindo a memória SRAM, *Static RAM* (Memória de Acesso Aleatório Estático), pois esta possuía um alto preço por ser bem mais elaborada, apresentando uma densidade menor e com isso um tempo menor de acesso. Com o passar do tempo a memória DRAM tornou-se padrão, ficando conhecida pela maioria dos usuários apenas pela sigla RAM, mas a memória SRAM ainda é utilizada pelos processadores em seu cache interno.[6]

Funcionamento da Memória

Os chips de memória RAM são bem simples, possuindo inúmeros transistores, e para cada transistor um capacitor. Quando um capacitor esta carregado eletricamente, temos um *bit* "1" e quando esta descarregado, temos um *bit* "0". Os transistores são responsáveis pela verificação de qual *bit* está armazenado em seu capacitor e pelo envio dessa informação ao controlador de memória. A memória RAM é considerada "volátil" devido ao fato do capacitor perder rapidamente sua carga e, desta forma, perder toda informação ali contida.[11]

As memórias utilizadas, hoje em dia, são altamente confiáveis, isso se deve ao fato dos sistemas possuirem um contador de memória que é responsável por verificar erros no momento em que o sistema inicia. Para a verificação de erros é utilizado o método conhecido como paridade.

Encapsulamentos de Memória

Podemos destacar quatro tipos de encapsulamentos principais de memória utilizados em computadores pessoais: DIP, SIPP, SIMM e DIMM [3]. Dentre eles, o mais utilizado é o encapsulamento conhecido como DIMM.

A memória DIMM (*Double In Line Memory Module*), recebe este nome devido ao fato de possuir contatos nos dois lados do módulo, diferente de seus antecessores que possuíam contatos em apenas um lado.

Esta memória possui três formatos, sendo os mais antigos os módulos de memória SDR SDRAM de 168 vias, logo após veio o módulo de memória DDR SDRAM, que possui 184 vias e, em seguida o módulo DDR2 SDRAM, que possui 240 vias. Maiores detalhes destes três formatos de memória podem ser encontrados no documento ***Forense Computacional em Memória Principal*** em [18].

B. Interferência da Temperatura Sobre o Armazenamento da Memória

Como visto anteriormente, os dados na memória são armazenados em capacitores. Capacitor é um dispositivo eletro-eletrônico que serve para armazenar energia elétrica no campo elétrico existente no seu interior [12]. Na memória principal, quando o capacitor está carregado, temos o *bit* "1" e quando está descarregado temos o *bit* "0".

Quando um módulo de memória é desligado, a energia armazenada nos capacitores é esgotada, daí o motivo da volatilidade da memória principal, todavia, os capacitores possuem uma característica importante, **sua capacitância** (capacidade de armazenamento elétrico) **sofre grande influência da temperatura**.

A capacitância de um capacitor é elevada com o aumento da temperatura, ou seja, a capacidade de manter a energia armazenada aumenta com o aumento da temperatura, da mesma forma que a capacitância diminui com a diminuição da temperatura.[9]

Este fato ocorre devido à constante dielétrica dos componentes do capacitor que aumenta (com a elevação da temperatura) ou diminui (com a redução da temperatura). Em geral, o comportamento da capacitância com relação à temperatura é especificado pelo próprio fabricante.

A temperatura também influencia na vida útil de um capacitor, por exemplo, um módulo de memória possui uma vida útil estimada de 1 a 5 anos de uso contínuo, essa vida útil pode ser aumentada em 100%, simplesmente, abaixando a temperatura interna da máquina em 10 ºC.[5]

C. Ferramentas Para Análise de Evidências

Conforme retromencionado, na parte de coleta de evidências, para realizar um trabalho de forense é extremamente importante que se tenha em mãos um conjunto de ferramentas apropriadas. Isto envolve *softwares* e dispositivos de *hardware* que venham a ser necessários. O profissional ou equipe responsável deve ter familiaridade com o material, devendo ser devidamente testadas e preparadas as ferramentas para evitar situações indesejadas.

O Aplicativo DD

O comando dd é um aplicativo comumente encontrado em sistemas Unix e Linux, mas também possui versões disponíveis para Windows. O dd é capaz de fazer cópias *bit*-a-*bit*, de dispositivos de bloco, criando um espelhamento perfeito de partições, discos ou arquivos. Sua sintaxe básica de uso é:

```
dd if=origem of=destino
```

Algumas opções disponíveis para uso em conjunto com o comando dd:

- **bs:** Tamanho do bloco;
- **ibs:** Tamanho do bloco de entrada;
- **obs:** Tamanho do bloco de saída;
- **count:** Número de blocos a copiar;
- **skip:** Número de blocos a pular no início da origem;
- **seek:** Número de blocos a pular no início do destino;
- **conv:** Conversão.

Helix

O Helix é uma distribuição Linux live cd, baseada no Knoppix. Ao inicializar é carregado um SO Linux completo, sem alterar dados em discos. É amplamente conhecida por conter várias ferramentas para análise forense, ferramentas para captura de imagem como o dd, mencionado anteriormente, e outras como Adepto, Air, LinEn e Retriever.

Possui um bom conjunto de ferramentas para análise (AutoPsy, pyflag, regviewer, hexeditor), antivírus (Clam-Av e F-prot) e *sniffers* entre outras ferramentas. O Helix disponibiliza também algumas dessas ferramentas em versão Windows, mas neste trabalho será usado como referência o live cd Linux.

Ao ser inicializado em sua opção padrão, é disponibilizado um ambiente de trabalho gráfico, com acesso fácil às ferramentas, cujas principais são:

- **Adepto:** Aquisição de imagens e gerar cadeia de custódia;
- **Air:** Interface gráfica para o dd;
- **Linen:** Ferramenta para captura de imagens da Guindance (desenvolvedora do Encase), permite a captura de imagens para análise no Encase;
- **Retriever:** Utilitário capaz de varrer discos e partições a procura de arquivos de imagens gráficas;
- **Autopsy:** Utilitário para análise forense de sistemas Windows e Linux;
- **pyFlag:** Utilitário para análise de logs;
- **Regviewer:** Navegador do registro do Windows;
- **Hexeditor:** Editor binário para leitura de arquivos em ASCII e hexadecimal;
- **XFCE Diff:** Utilitário gráfico para comparação de arquivos.

O Utilitário MDD

O programa mdd é uma ferramenta produzida e disponibilizada gratuitamente pela empresa ManTech International Corporation©. Ele é capaz de capturar imagens da memória RAM em sistemas operacionais Windows. O Live CD do Helix, anteriormente citado, contém também uma cópia deste programa.

Sintaxe de linha de comando para utilização do mdd:

```
mdd -o arquivo-de-saida
```

O Comando Strings

O comando strings é capaz de varrer um arquivo binário, extraindo de seu conteúdo seqüências de caracteres que podem ser impressos com letras do alfabeto e símbolos utilizados na computação. Sua saída traz as *strings* já em formato ASCII ou UNICODE.

Sintaxe do comando strings:

```
strings arquivo-binário
```

V. Estudo de Caso

O trabalho de forense computacional é realizado, em sua maioria, em memória secundária (HD, CD, DVD, Pen drive, etc...), e não é atribuído muito valor à memória principal, devido a sua volatilidade. Sendo assim, muito se perde em qualidade em uma investigação forense computacional. Portanto, seria de grande valor se o conteúdo da memória RAM pudesse ser recuperado mesmo após o desligamento do equipamento.

O conceito amplamente divulgado é o de que, após a interrupção do fornecimento de energia, todo o conteúdo de memória RAM é perdido, mas sabe-se que os *bits* são armazenados por capacitores dentro das células de memória e que, quando interrompida a energização externa de um capacitor, ele pode manter a carga armazenada por um período. Sabe-se, também, que os capacitores possuem uma característica importante, sua capacitância sofre grande influência da temperatura. Com isso, é possível que mesmo após o desligamento de um equipamento, parte do conteúdo de sua memória RAM continue preservado por um período de tempo.

O que se pretende com este trabalho é mostrar e provar que a memória principal pode ser muito importante na análise forense, para isso, será demonstrado, através de um estudo de caso, que a volatilidade da memória principal é questionada. Será testada a persistência de dados na memória "volátil" de computadores, mesmo após a interrupção do fornecimento de energia. Pretende-se levantar dados estatísticos sobre a permanência de informações após interrupções forçadas de energia elétrica. Para isso, será trabalhada a carga de dados pré-determinados na memória do equipamento com um conjunto de palavras específicas.

A. Realização dos Testes

A idéia fundamental foi inicializar o equipamento com um sistema Linux enxuto, ou seja, que consuma pouco espaço na memória ao ser inicializado. Após a finalização da carga

normal do SO, foi verificado o status de utilização da memória através do comando **"top"**. Nosso interesse estava na área livre na memória, a qual pretende-se marcar. A marcação foi feita escrevendo um referido conjunto de palavras repetidamente até preencher totalmente a memória física. Para carregar na memória o referido conjunto de palavras, foi usado um arquivo texto gerado previamente. Esse arquivo, gerado com o auxílio de um *Shell Script*, contém um conjunto de palavras replicada diversas vezes, gerando um volume de dados próximo ao espaço livre na memória.

Exemplo do arquivo gerado contendo o conjunto de palavras de marcação:

```
"teste TCC memoria 13/01/2009"
"teste TCC memoria 13/01/2009"
"teste TCC memoria 13/01/2009"
…
```

Configuração do equipamento utilizado nos testes:

```
Processador: Intel(R) Pentium(R) DualCPU E2160 1.8 GHz
Memória: 1 GB DDR2 667 MHz
```

Sistemas operacionais utilizados nos testes:

```
Linux: Slackware kernel 2.6.24.5-smp
Windows: Microsoft Windows XP SP2
```

A carga dos dados foi feita abrindo o arquivo gerado com um editor de texto, que em nosso caso foi utilizado o **"vi"**. É possível acompanhar a diminuição gradual do espaço livre na memória através do comando **"top"**. Para referência e comparações, captura-se uma cópia *bit-a-bit* de toda a memória logo após a carga.

Com o programa **"dd"** (foi utilizado o programa **"mdd"** para o teste realizado em ambiente Windows) copiou-se o conteúdo do dispositivo de bloco **"/dev/mem"** para um arquivo em disco. Em seguida, o equipamento foi fisicamente desligado, interrompendo-se o fornecimento de energia e, assim, permanecendo por períodos de tempo de um, cinco, dez e trinta minutos. Depois o equipamento foi ligado e após a finalização do *boot*, uma nova cópia *bit*-a-*bit* do conteúdo da memória foi gerada.

Copia-se o conteúdo da memória com o dd:

```
No Linux: dd if=/dev/mem of=/arquivo-dump bs=1024
No Windows: mdd.exe –o arquivo-dump
```

Agora que se tem os *dumps* (arquivo contendo os mesmos dados de uma memória, volátil ou não) das memórias originais, realizados logo após a carga dos dados na memória, e os *dumps* das memórias após realizadas as interrupções de energia, a próxima etapa é a analise do conteúdo desses *dumps* para tentar localizar evidências do conjunto de palavras intencionalmente carregada. Para essa análise, utilizou-se o comando **"strings"**, que identifica em arquivos binários seqüências de dados que sejam entendidos.

A saída do comando **"strings"** foi direcionada para arquivos em disco. Esses arquivos contêm todos os conjuntos de palavras identificados dentro dos arquivos de *dump* de memória, agora já convertidas para caracteres ASCII, facilitando o trabalho de identificação dos dados.

Para a extração de seqüências de texto a partir dos aquivos binário com *dumps* da memória, usa-se o comando strings:

```
#strings arquivo-dump > arquivo-destino-strings
```

Pode-se, então, analisar esses novos arquivos contendo apenas seqüências de texto, que foram identificadas dentro dos *dumps*. Esses novos arquivos são transformados em um formato que podemos compreender, o formato ASCII. Assim, pode-se buscar o que se deseja com associação de comandos como **"cat"**, **"grep"** e **"wc"**.

Para se contar as linhas onde há a ocorrência de uma determinada palavra ou conjunto de palavras dentro de um arquivo, utilizou-se:

```
#cat arquivo-destino-strings | grep "palavra/conjunto de palavra desejada" | wc -l
```

B. Resultados dos Testes

Neste trabalho, foram realizados cinco conjuntos de testes. Primeiramente foram colhidos os dados após reinicialização do sistema, em seguida foi mantida a interrupção da energia em intervalos que variaram entre um (1) minuto, cinco (5) minutos, dez (10) minutos e trinta (30) minutos.

No primeiro teste, nomeado *"Reset"* para facilitar na identificação dos resultados, após a carga de memória, o equipamento foi reinicializado fisicamente, e no *boot* seguinte gerado o *dump*. Esse primeiro teste serviu como referência para se verificar o comportamento dos dados na memória no *boot* subsequente. Nesses testes foram utilizados o SO Linux e Windows, onde foi constatado que no Windows a memória foi, provavelmente, limpa no *boot* posterior à reinicialização, não sendo possível identificar vestígios do conjunto de palavras de teste no *dump* da memória após a reinicialização. Já no Linux, é possível identificar vestígios do conjunto de palavras, tanto completa como em partes.

Nos testes seguintes, após a carga da memória com o conjunto de palavras, o equipamento teve o fornecimento de energia interrompido. A interrupção foi mantida por intervalos de tempo pré-determinados, de um, cinco, dez e trinta minutos.

O procedimento de carga dos dados na memória foi exatamente igual ao realizado no teste de reinicialização.

Depois de cada intervalo, o equipamento era reinicializado e em seguida era feita à coleta da temperatura pela BIOS e gerado um *dump* da memória para análise. Os dados estatísticos dos testes seguem nos gráficos a seguir. A legenda do lado direito do gráfico representa a medida da temperatura, em °C, fornecida pela BIOS referente a CPU.

Gráfico 1: Resultado de ocorrências para a string completa.

Gráfico 2: Resultado de ocorrências para a palavra "teste".

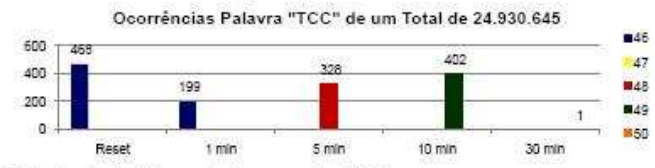

Gráfico 3: Resultado de ocorrências para a palavra "TCC".

Gráfico 4: Resultado de ocorrências para a palavra "memoria".

Gráfico 5: Resultado de ocorrências para a palavra "13/01/09".

Os resultados dos testes foram bastante promissores. Como o objetivo inicial era provar a permanência dos dados após o desligamento do equipamento, ou seja, a não volatilidade da memória principal (RAM), com os dados apresentados, pode-se afirmar que houve êxito. **Com isso, fica evidente que a memória principal (RAM) pode ser utilizada em uma análise forense computacional.**

Além do êxito em confirmar por meio de dados a proposta dos trabalhos realizados, foram constatados outros fatos. Como pode ser visto nos gráficos, realmente a temperatura influenciou os dados na memória, pois apesar da máquina ficar desligada mais tempo foi possível obter mais informações na memória principal. Este fato é justificado pelo aumento na temperatura das máquinas, comprovando as afirmações apresentadas em [9].

Observa-se, também, nos gráficos que há uma variação muito pequena entre os percentuais de recuperação e isso fica mais claro no gráfico a seguir, contendo a evolução do valor do índice de recuperação completa, sendo que após trinta minutos não foram encontradas mais ocorrências do conjunto de palavras por inteiro, apenas poucos fragmentos.

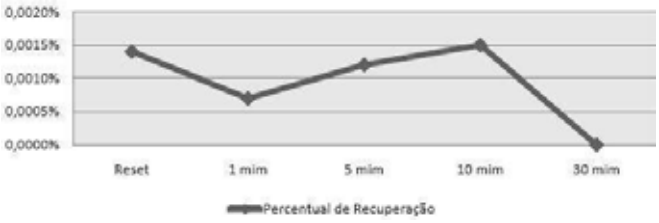

Gráfico 6: Percentual de recuperação de uma string completa.

Comparando os resultados dos testes de interrupção de fornecimento de energia entre si, e considerando-os de maneira geral, incluindo o teste de reinicialização, pode-se deduzir que a maior perda de dados foi ocasionada pelo processo de carga do SO na memória principal durante os testes. Portanto, para a captura de dados da memória RAM após o desligamento do equipamento, é desejável a inicialização através de um SO Linux, sendo este o mais enxuto possível para minimizar o risco de sobrescrita dos dados.

Outro aspecto que pode ser avaliado em trabalhos futuros é a influência da temperatura na persistência dos dados na memória após o desligamento, pois em temperaturas maiores, os capacitores que compõem as células de memória tem sua capacitância aumentada. Isso foi comprovado em partes, já que no início de nossos testes a temperatura medida pela BIOS era de 46° C e no final dos testes essa temperatura era de 50° C, ou seja, na medida em que o trabalho de laboratório estava sendo realizado, nos períodos que a máquina estava ligada, a temperatura interna da máquina aumentava e, assim, mais dados puderam ser recuperados, com exceção do teste de trinta minutos, onde os dados recuperados da memória foram praticamente nulos.

VI. Conclusão

A forense computacional é uma área que ainda tem muito a desenvolver, inovar e aperfeiçoar as tecnologias e métodos para se obter mais e melhores evidências. Por ser uma área criada recentemente, ainda existem poucos profissionais capacitados que conhecem e seguem os procedimentos já aprovados pela comunidade científica da área, além de existir uma limitada quantidade de *softwares* e *hardwares* disponíveis para a realização de perícias nos equipamentos.

Com a necessidade e iniciativa de se atualizar as leis brasileiras para um melhor entendimento jurídico sobre os crimes digitais, indiscutivelmente haverá uma crescente demanda por peritos em forense computacional, necessários para provar que os atos criminosos previstos em lei foram cometidos, com evidências autênticas e confiáveis, dando um melhor suporte para o tribunal não cometer erros.

É necessária uma maior atenção por parte dos profissionais da área de forense computacional em relação à memória

principal dos equipamentos periciados, que geralmente ou são desprezadas ou simplesmente ignoradas, por achar que terão toda a evidência necessária nos dispositivos de memória secundária ou então porque os equipamentos provavelmente foram desligados ou reiniciados por terceiros. Mas, de acordo com este estudo, foi percebido que, mesmo após a ocorrência destas interações, dados ainda podem residir na memória RAM do computador, sendo uma preciosa fonte de evidências, pois, o conteúdo delas não possui proteções de segurança e demonstram o comportamento do sistema no momento em que ele acessou a memória para gravar dados.

É importante lembrar que a memória RAM está, também, presente em outros dispositivos, tais como, palmtops, computadores de bordo de carros, além de outros equipamentos que fazem parte do nosso cotidiano.

Há, agora, uma necessidade de se estudar melhor como tornar o percentual de persistência de dados na memória maior, propondo técnicas que levem em consideração a temperatura, a tecnologia e melhores *softwares* envolvidos, para se ter uma melhor opção na busca de evidências digitais, aumentando a veracidade das conclusões obtidas nas perícias realizadas. Deve-se verificar, também, o comportamento da memória de swap do sistema operacional, bem como a memória RAM se comporta em outros dispositivos que não sejam computadores.

Referências bibliográficas

[1] ALECRIM, Emerson. **Memória DDR (Double Data Rating).** Disponível em: <http://www.infowester.com/memddr.php>. Acesso em: 16 jan. 2009;

[2] ALECRIM, Emerson. **Memória DDR2.** Disponível em: <http://www.infowester.com/memddr2.php>. Acesso em: 16 jan. 2009;

[3] ALECRIM, Emerson. **Memórias ROM e RAM.** Disponível em: <http://www.infowester.com/memoria.php >. Acesso em: 21 nov. 2008;

[4] COLETTA, Alex de Francischi. **Gerenciamento de Memória.** Disponível em: <http://www.alexcoletta.eng.br/2008/gerenciamento-de-memoria/>. Acesso em: 07 out. 2008;

[5] Guia do Hardware.net. **Capacitor Eletrolítico.** Disponível em: <http://www.guiadohardware.net/termos/capacitor-eletrolitico>. Acesso em: 24 jan. 2009;

[6] Guia do Hardware.net. **Memória RAM.** Disponível em: <http://www.guiadohardware.net/termos/memoria-ram>. Acesso em: 07 out. 2008;

[7] LEMOS, Ronaldo, BOTTINO, Thiago, SOUZA, Carlos Affonso Pereira de, BRANCO, Sérgio, PARANAGUÁ, Pedro, MIZUKAMI, Pedro Nicoletti, MAGRANI, Bruno, MONCAU, Luiz Fernando. **Comentários e Sugestões sobre o Projeto de Lei de Crimes Eletrônicos (PL n. 84/99).** 2008. 21p. Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, Rio de Janeiro;

[8] LINHARES, Daniel. **Aplicação de Técnicas de Forense Computacional e Respostas a Incidentes na Internet.** 2004. 166 p. Brasília;

[9] MEHL, Ewaldo L. M. **Capacitores Eletrolíticos de Alumínio: Alguns cuidados e considerações práticas.** Disponível em: <http://www.eletrica.ufpr.br/mehl/downloads/capacitores.pdf>. Acesso em: 24 jan. 2009;

[10] MONTOVANI, Glenio. **Ferramentas para análise forense aplicada à informática.** 2008. 108p. Monografia (Pós Graduação em Segurança da Informação). Universidade Salgado de Oliveira, Goiânia;

[11] MORIMOTO, Carlos E. **Memória RAM.** Disponível em: <http://www.guiadohardware.net/tutoriais/memoria-ram/>. Acesso em: 07 out. 2008;

[12] MUSSOI, Fernando Luiz Rosa, VILLAÇA, Marco Valério. **Capacitores.** 2000. 39p. 3ª Edição, CEFET/SC, Florianópolis;

[13] REIS, Marcelo Abdalla dos, GEUS, Paulo Lúcio de. **Análise Forense de Intrusões em Sistemas Computacionais: Técnicas, Procedimentos e Ferramentas.** Instituto de Computação - Universidade Estadual de Campinas, Campinas;

[14] TANENBAUM, Andrew S., WOODHULL, Albert S. **Sistemas Operacionais – Projeto e Implementação.** Tradução: Edson Furmankiewicz. 2ª Edição . Porto Alegre: Bookman, 2000. 341p;

[15] TechFAQ. **O que é SDR SDRAM?** Disponível em: <http://pt.tech-faq.com/sdr-sdram.shtml>. Acesso em: 16 jan. 2009;

[16] TORRES, Gabriel. **Entenda às Memórias DDR2.** Disponível em: <http://www.clubedohardware.com.br/artigos/1046>. Acesso em: 17 jan. 2009;

[17] TYSON, Jeff. **Como funciona a memória do computador.** Disponível em: <http://informatica.hsw.uol.com.br/memoria-do-computador.htm>. Acesso em: 16 jan. 2009;

[18] LISITA, Bruno L., MOURA, Thiago S. M. e PINTO, Tiago J. **Forense Computacional em Memória Principal**. Trabalho de conclusão de curso de Pós-graduação em Segurança da Informação na FATESG/SENAI/GO.