Brazilian Journal of Forensic Sciences, Medical Law and Bioethics

Journal homepage: www.ipebj.com.br/forensicjournal

Análise Forense Computacional de Ambientes Virtualizados – Abordagens de *Live Analysis* e de *Dead Analysis*

Computational Forensic Analysis of Virtualized Environments – *Live Analysis* and *Dead Analysis* Approaches

Deivison Pinheiro Franco[1]

[1] *Graduado em Processamento de Dados. Especialista em Redes de Computadores, em Suporte a Redes de Computadores e em Ciências Forenses (Ênfase em Computação Forense). Analista Pleno de TI do Banco da Amazônia. Professor em várias faculdades das disciplinas: Informática Forense, Segurança da Informação, Redes, SO e Arquitetura de Computadores. Perito Forense Computacional Judicial (Assistente Técnico), Auditor de TI e Pentester com as certificações: CEH - Certified Ethical Hacker, CHFI - Certified Hacking Forensic Investigator, DSEH - Data Security Ethical Hacker, DSFE - Data Security Forensics Examiner, DSO - Data Security Officer e ISO/IEC 27002 Foundation.*

Received 12 October 2012

Resumo. Esse é um estudo a respeito de análise forense computacional de ambientes virtualizados. Apresenta uma visão sobre ambientes virtualizados e suas implicações em análises forenses computacionais, mostrando seus componentes, conceitos e aspectos de segurança, abrangendo os avanços tecnológicos das ferramentas de virtualização, dos métodos e das questões de investigação forense digital. Para isso, foi mostrada a interação dos processos de virtualização com os processos de análise forense computacional; indicados os problemas (fragilidades à luz forense) da virtualização; e se discutiu métodos, bem como questões de análise forense computacional desse tipo de ambiente.

Palavras-Chave: Ambientes Virtualizados; Máquinas Virtuais; Computação Forense; Segurança; Crimes Cibernéticos.

Abstract. This is a study about computational forensic analysis of virtualized environments. It presents an insight into virtualized environments and their implications in forensic computing, showing its components, concepts and aspects of security, including technological advances of virtualization tools, methods and issues of digital forensics. Therefore, it was shown the interaction of processes with the processes of virtualization

http://dx.doi.org/10.17063/bjfs2-1-y201214

computer forensics; indicated problems (weaknesses to light forensic) virtualization, and discussed methods as well as computer forensics analysis questions of this kind of environments.

Keywords: Virtualized Environments; Virtual Machines; Forensic Computing; Security; Cybercrime.

1. Introdução

O crescimento e a evolução dos ambientes e das infraestruturas de Tecnologia de Informação (TI) trazem a necessidade de alternativas para simplificação, aumento de produtividade e redução de custos. Para esse fim, a virtualização se mostra como uma das melhores e mais eficientes opções a serem adotadas. Contudo, sua técnica cria novos desafios e dificuldades às análises forenses computacionais[1].

Nesse contexto, e ainda para Morrison[2], a virtualização surge como uma forma de esconder e melhor distribuir e utilizar as características e recursos físicos de uma plataforma computacional, por meio de um hardware virtual, emulando um ou mais ambientes isolados, virtualizando-se desde seu hardware a sistema operacional e aplicativos.

Ante ao exposto e para Marins[3] é de vital importância que se enfoque especial atenção aos quesitos de segurança inerentes e necessários em ambientes virtualizados, de modo a se possibilitar uma eficiente auditoria e processo de análise forense computacional em casos de fraudes e/ou ilícitos que sejam executados nesses tipos de ambientes. Dessa forma, pretende-se prevenir, restaurar e analisar vestígios e evidências computacionais, tanto os componentes virtuais ou físicos, quanto dados que foram processados ou acessados eletronicamente e armazenados.

2. Análise Forense Computacional de Ambientes Virtualizados

A proposta da virtualização é adequada para se trabalhar com imagens virtuais de máquinas reais sem modificá-las. Antigamente esse processo requeria ao perito clonar o hardware (HD), coloca-lo em um novo equipamento e inicializá-lo. Assim sendo, quando da primeira inicialização, o perito ainda não podia ter certeza se a imagem clonada estaria adequada à investigação. Dessa forma, sempre que houvesse qualquer suspeita de contaminação do clone, tornava-se necessário refazê-lo a partir de uma cópia válida. Isso tudo era um processo demorado e que

poderia ser facilmente contestado, uma vez que a integridade dos dados poderia ser perdida e/ou questionada.

Os sistemas operacionais e aplicativos executados em ambientes virtualizados deixam diferentes tipos de vestígios computacionais para serem analisados, o que resulta em novas evidências e procedimentos na condução de uma investigação quando da ocorrência de um delito digital. Fator este que se agrava devido à falta de técnicas e/ou procedimentos direcionados à execução de sua análise forense computacional.

Baseando-se em Melo[4], em Ormandy[5] e em Barrett[6], observa-se que a conceituação da perícia forense tradicional foi elaborada para tratar eventos que ocorrem no mundo real. No mundo virtual, sua demanda é muito recente, ainda mais em se tratando de ambientes virtualizados, isto é, um mundo virtual dentro de um mundo virtual, e por falta de técnicas forenses específicas para estes casos, procura-se adaptar métodos existentes para analisar as situações ocorridas nesse tipo de ambiente.

Com o avanço da tecnologia, várias soluções surgiram para diminuir custos e aumentar a disponibilidade dos sistemas e serviços oferecidos pelo setor de TI. Uma dessas soluções é a virtualização de sistemas operacionais completos, o que possibilitou uma diminuição nos gastos com hardware.

A virtualização trouxe um novo paradigma computacional, completamente diferente do anterior, onde não é possível se ter acesso à memória física de sistemas virtualizados que compartilham os mesmo dispositivos de hardware. Nesse cenário, como tudo é virtualizado, os processos do sistema também o são, assim como os discos e mídias.

Nesse novo paradigma, nem aos servidores com os sistemas virtualizados há acesso físico, e como os crimes e comprometimento de informações não são prerrogativas apenas de sistemas tradicionais, essas mesmas questões também ocorrem em máquinas e ambientes virtualizados. Sendo que o problema nesse caso, é que se torna necessário entender como essa tecnologia funciona, como é possível realizar a análise de seus dados e, principalmente, como utilizar essa tecnologia em benefício próprio como à luz da forense computacional, já que antigamente, o perito tinha que fazer uma nova imagem forense sempre que houvesse risco de que a cópia que estava periciando pudesse ter sido modificada.

Com a virtualização há a possibilidade de modificação da imagem periciada a qualquer tempo. Nas melhores práticas para as análises forenses computacionais de

ambientes virtualizados o perito tem que fazer dois clones do disco original para se proceder às fases propostas para a coleta de evidências e perícia.

Adaptando-se as fases de um processo de computação forense tradicional, é possível incluir as etapas e o cenário para a análise forense computacional de ambientes virtualizados, delimitando-as em: Acesso, Coleta, Análise e Relatório. A primeira destina-se ao acesso efetivo do perito ao ambiente a ser analisado. A segunda à produção de imagens, para serem usadas na perícia (tanto virtual quanto tradicional). A terceira à análise efetiva das imagens geradas pelo perito. Finalmente, a quarta corresponde à elaboração de relatórios (laudo) acerca das análises realizadas no ambiente.

Ante ao exposto, é necessário considerar alguns aspectos da computação forense que são afetados pela virtualização, pois existem vários problemas com a investigação digital dentro de ambientes virtualizados. São eles:

- ✓ A aquisição de dados dentro do ambiente;
- ✓ Como coletar dados;
- ✓ Quais dados coletar;
- ✓ Como lidar com os dados que normalmente estão sempre em “movimento”;
- ✓ Como respeitar a privacidade dos outros hosts que não estão sob investigação.

Assim sendo, adiante irá se explicar o processo de transformação de evidências digitais ocorridas em ambientes virtualizados em algo que um perito possa usar e analisar com confiança. Destarte, ao usar uma máquina virtual, o conteúdo da máquina pode ser visto da mesma forma que o suspeito viu. Sendo que ainda será discutido o conceito de “melhores evidências”, bem como a aceitabilidade das provas obtidas a partir de instâncias virtuais do computador de um suspeito, descrevendo um método proposto que combina métodos tradicionais com a tecnologia virtual para usufruir dos benefícios da virtualização e ainda atender aos rigores esperados pela investigação forense quando da ocorrência de delitos em ambientes virtualizados.

3. Análise Forense Computaconal de Ambientes Virtualizados – Abordagem de *Live Analysis* (*In Vivo*)

Por um longo tempo, a análise forense computacional utilizava apenas unidades estáticas ou “mortas”. De fato, em muitos casos, esse ainda é o principal método para se encontrar evidências. Nesse tipo de análise forense, muitas vezes as

evidências encontradas são escassas e, enquanto a tecnologia avança, a análise forense computacional de ambientes virtualizados mortos (desligados) confronta-se com desafios como redes mais complexas, maior capacidade de armazenamento e criptografia.

Com o aumento da quantidade de evidências recuperáveis, as investigações do tipo *in vivo*, ou *live*, estão se tornando cada vez mais comuns. De fato, muitas organizações de grande porte, especialmente as vinculadas ao governo, alteraram a maior parte de seus tipos de análise forense computacional para a *live analysis*, já que em uma grande empresa, preservação de dados pode ser bastante onerosa, uma vez que as evidências obtidas das imagens completas dos discos de vários funcionários podem exigir vários terabytes de armazenamento.

Ante ao exposto, recomenda-se a cópia (não imagem) dos arquivos que montam e carregam a máquina virtual suspeita, em mídias que possam ser asseguradas pela cadeia de custódia. Essa abordagem pode ser empregada para qualquer caso exceto aqueles em que o servidor de virtualização está sendo usada para influenciar ou corromper as máquinas virtuais (VMs).

O arquivo de imagem usado pela VM contém todo o espaço alocado e não alocado na máquina físico, logo se a atividade suspeita estiver no computador original, cópias do arquivo de imagem da máquina virtual, bem como os arquivos associados a ela são suficientes para a investigação forense. No entanto, se houver qualquer possibilidade de corrompimento ou influência externa à VM afetar seus arquivos, estes devem ser visualizados em vez de copiados. Contudo, se o tamanho de alocação da máquina virtual (tamanho do arquivo que monta a máquina virtual) diminuir ao longo do tempo, pode ser que não seja necessário mais do que apenas o sistema de arquivos existentes na VM, dependendo das especificidades de cada caso.

Como há uma grande mudança no cenário da computação atual, com a TI verde impulsionando cada vez mais o conceito e a implementação da consolidação de hardware, as organizações têm, cada vez mais, migrado para ambientes virtualizados, o que propicia chances para se proceder a análises forenses computacionais do tipo *live* neste tipo de ambientes. Entretanto, há algumas questões específicas relacionadas com esses ambientes que um perito deve estar ciente de quando da condução de uma análise in vivo dos mesmos.

3.1 Fundamentos

Todas as análises forenses computacionais exigem que as metodologias utilizadas para coletar evidências sejam sólidas e assegurem que as provas serão admissíveis em um tribunal. Metodologias forenses computacionais também são baseadas em verificação e repetição. Embora a forense computacional *in vivo*, ou *live*, esteja se tornando mais aceitável, ainda existem algumas questões relacionadas com este tipo de técnica. A questão principal é que investigações do tipo *live* mudam o estado do sistema investigado e seus resultados não podem ser repetidos. Qualquer mudança do estado do sistema e inconsistências de verificação e repetição das evidências vai de encontro aos princípios aceitos no meio da forense computacional. Até agora, grandes avanços têm sido feitos em relação às limitações impostas na admissibilidade de evidências coletadas através da técnica do tipo *live*, mas este tipo de coleta empregada em ambientes virtualizados pode ser um pouco mais complicado.

Análises forenses computacionais do tipo *live* ajudam a proteger evidências digitais sensíveis e facilmente alteráveis, podendo ser realizadas de diferentes maneiras. Muitos pacotes comerciais para forense computacional oferecem a capacidade de controle e monitoramento do ambiente de trabalho (virtualizado ou não). Um pacote pode ser adquirido e os dados que trafegam no ambiente podem ser coletados em tempo real. Outros pacotes permitem coleta e análise *in vivo* através de navegadores *web*. Esses aplicativos oferecem os mesmos recursos que um *applet* instalado, mas são usados sob demanda ou em um incidente notificado pelo monitoramento. Finalmente, há a resposta da primeira análise, onde as coletas in vivo são feitas mediante a notificação de um incidente.

Independentemente do método utilizado para a coleta e análise, o princípio da análise forense computacional *in vivo* é baseado na premissa da coleta de dados a partir de um sistema em execução (ligado) a fim de se recolher informações pertinentes e que não estejam disponíveis em análises do tipo *dead* (com o ambiente desligado). Dessa forma, as informações recolhidas nessa técnica normalmente consistem do sistema de dados voláteis, tais como memória, aplicações e processos em execução, bem como portas abertas, soquetes e conexões ativas.

Ao criar uma imagem forense é necessário se provar que a imagem é uma cópia exata, ou documentar e explicar todas e quaisquer diferenças e como ocorreram. Há a possibilidade de se criar uma imagem forense e, em seguida,

convertê-la ou copiá-la em um sistema virtual. Contudo, isso se torna um problema quando o caso sob investigação demanda a análise de muitos discos. Porém, já há um novo formato de imagem chamado *Advanced Forensic Format* que foi projetado para ajudar o perito a lidar com unidades de disco e volume de dados muito grandes, através da alocação de metadados sobre uma unidade com os dados do disco e segmentando-a em partes gerenciáveis.

Como dito antes, a forense computacional tradicional obriga a criação de uma imagem completa do disco, tornando quase impossível de se realizar uma perícia em terabytes de dados.

Para resolver esse tipo de situação, Bawcom[7] propõe a utilização de duas técnicas - a *Live Response* e a *Live Acquisition*. Na primeira, o perito acessa um sistema em execução e coleta informações voláteis e não voláteis, sendo que uma das formas mais práticas para se guardar as informações voláteis, além da utilização de ferramentas comerciais, é o uso de um sistema remoto forense, um CD/DVD inicializável, ou um cartão USB. Na segunda, o perito cria uma imagem do disco rígido enquanto o sistema ainda está em execução. Estas duas técnicas desafiam as melhores práticas para solução de problemas que não podem ser resolvidos usando-se as técnicas tradicionais de computação forense.

Ante ao exposto, há três regras que devem ser observadas para se garantir a confiabilidade de evidências digitais: devem ser produzidas, mantidas e utilizadas em um ambiente normal; devem ser autenticadas por um perito; e devem ser a melhor evidência disponível.

A RFC 3227 traz orientações e considerações legais para a coleta e arquivamento de evidências e define as melhores práticas para resposta a um incidente de segurança, descrevendo os procedimentos de coleta em ordem de volatilidade, do mais volátil para o menos volátil e preconiza que uma evidência digital deve ser:

1. Admissível - obedecer a normas legais;
1. Autêntica - probatória para o incidente;
2. Completa - contar a história toda e não apenas uma determinada perspectiva;
3. Confiável - não deve haver dúvidas sobre autenticidade e veracidade de sua coleta;
4. Acreditável - crível e compreensível.

Para fins de atendimento eficiente dessas regras e orientações, bem como para a redução dos desafios inerentes às ferramentas forenses, o NIST produziu um conjunto de especificações de teste (especificações de ferramentas para imagens digitais), destinados a serem utilizados na validação de ferramentas usadas para criar imagens forenses. Essas especificações garantem que as ferramentas para a criação de imagens de discos produzam imagens forenses confiáveis.

Como os ambientes virtualizados estão se tornando cada vez mais comuns, em uma análise forense computacional in vivo, dependendo das ferramentas utilizadas, o ambiente virtual pode ou não ser capturado e analisado de modo a atender o que preconiza a RFC 3227. Para isso, imagine-se um cenário no qual uma organização utiliza uma solução empresarial que inclui uma ferramenta que monitora as estações de trabalho de seus usuários através de um programa de monitoração instalado. A intenção desse ambiente é fornecer aos seus administradores a capacidade de monitorar as máquinas da rede, o que pode ser feito em modo silencioso colocando-se os programas de monitoramento em um servidor sem se alertar os usuários do processo, permitindo que o monitoramento seja executado sem ser percebido e transformando-o em uma ferramenta para fins forenses computacionais. Contudo, mesmo que o monitoramento seja silencioso, se o usuário utiliza um ambiente virtual que usa a placa de rede do host, o tráfego pode ser analisado, mas o monitoramento não seria capaz de esmiuçar o ambiente e se restringiria a mostrar apenas as atividades do host físico e não do virtual.

Esse tipo de cenário foi testado com várias ferramentas, sendo que sua maioria foi ineficiente ao analisar ambientes virtualizados, quando da análise do tráfego de rede e endereçamento IP, sendo que o monitoramento reconhece o ambiente virtual, mas não pode ser nem instalado e nem executado nesse tipo de ambiente. Entretanto, esse é o resultado mais promissor, pois a ferramenta reconhece o ambiente virtual, uma vez que esses tipos de monitoramentos são projetados para funcionar interagindo entre o hypervisor e o host.

O avanço das técnicas e tecnologias de virtualização, bem como a disseminação da implantação de ambientes virtualizados, traz consigo também o avanço das ferramentas de monitoração desses tipos de ambientes, o que significa que a evolução e aperfeiçoamento das análises forenses dos mesmos irão progredir significativamente, já que todos os desenvolvimentos recentes para seu gerenciamento provisionamento e monitoramento propiciam aos peritos computacionais forenses formas mais concretas para se encontrar evidências.

Entretanto, a combinação da análise forense com ambientes virtualizados deve ser certificada acerca da capacidade de monitoramento das ferramentas para este tipo de ambientes, sendo que outro aspecto interessante é acompanhar o funcionamento da monitoração da VM de máquina para máquina.

Além de ferramentas comerciais, há muitas ferramentas de código aberto para monitoramento e análise de ambientes e máquinas virtuais, como o *Netcat*, e sua versão de criptografia, o *Cryptcat*, por exemplo. Ambas são gratuitas e usadas, além do monitoramento, para criação de imagens forenses de confiança entre o ambiente alvo e a estação forense.

Outra ferramenta de código aberto é o *Forensic Server Project*, que pode ser usado para coleta forense remota. Há, ainda, ferramentas inicializáveis através de CD/DVD, dentre as quais se podem citar o *DFLCD* e o *Knoppix STD*. Há muitas ferramentas disponíveis que propiciam condições para a análise forense computacional *in vivo* e que podem ser utilizadas para a investigação em ambientes virtualizados. Os avanços na capacidade de armazenamento de dados que uma unidade removível pode suportar, bem como sua velocidade de leitura e escrita e, ainda, sua a possibilidade de inicialização, fazem deste tipo de mídia atraentes para ferramentas de análise forense *in vivo*.

3.2 Artefatos e Evidências

Em uma análise forense computacional de ambientes virtualizados *in vivo*, há muitas semelhanças nos tipos e padrões de dados coletados em relação a um ambiente físico, pois em alguns aspectos, as evidências serão as mesmas tanto em um ambiente físico quanto em um ambiente virtual, tais como: usuários logados, portas abertas, processos em execução, informações de sistema e de registro e dispositivos conectados.

Na condução de uma análise forense computacional de ambientes virtualizados *in vivo*, algumas considerações adicionais são pertinentes para a validação do tipo de ambiente como: saber se o ambiente é físico ou virtual, saber se há virtualização de hardware, de software ou ambas, saber se existem endereços MACs, bem como unidades de hardware específicos e identificáveis. Esses itens podem parecer sem importância, mas podem afetar o resultado de um caso.

3.3 Arquivos de Processos e Portas

Em qualquer análise forense computacional de ambientes virtualizados *in vivo*, é importante se capturar suas portas abertas e serviços, dadas as particularidades de cada ferramenta de virtualização. Contudo, as coisas nem sempre são como parecem, logo, é importante que o perito proceda a análise de processos e portas com cuidado.

3.4 Arquivos de Log

A maioria dos fornecedores de virtualização já está provendo gerenciamento centralizado de recursos para máquinas virtuais, bem como suporte para SNMP e WMI, porém a padronização de logs remotos não está completamente perfeita ainda.

3.5 Uso de Memória

A análise da memória é um dos principais componentes de uma investigação do tipo *in vivo*. Quando uma máquina virtual é criada, a memória é alocada a ela. Nesse processo, partes da memória disponível no computador físico (memória real) são definidas (alocadas) para uso de cada máquina virtual. Dessa forma, o sistema operacional (SO) anfitrião (real) possibilita que seu gerenciador de memória defina o swap de memória física (RAM) para as máquinas virtuais alocadas na máquina real.

Alterações nas configurações de memória afetam diretamente as máquinas virtuais e o desempenho do sistema. Deve-se observar a limitação do total da quantidade de memória RAM alocada para as máquinas virtuais, a fim de que elas não consumam todo este recurso e façam com que o host entre em colapso.

Como regra geral, o total de memória de todas as máquinas virtuais em execução junto ao consumo de todos os processos não pode ser maior do que a quantidade de memória física do hospedeiro (máquina real), excluindo-se a memória adicional reservada ao host para seu funcionamento correto, enquanto as máquinas virtuais estiverem em execução.

A parte de memória reservada depende do sistema operacional hospedeiro e da quantidade de memória disponível no computador físico. Embora a quantidade de memória RAM utilizada possa ser reservada, a memória não é alocada antecipadamente e todo o restante não utilizado fica disponível para uso de outras aplicações, caso as VMs não o estejam o utilizando. No entanto, se toda a memória

RAM estiver em uso pelas VMs, apenas o SO anfitrião ou qualquer outra aplicação sua pode usá-la.

A sobrecarga de VM varia de acordo com o tamanho do disco e a memória alocada (tanto real quanto fisicamente). A fim de se evitar que isso ocorra, as seguintes opções podem ser utilizadas como referência:

5. Colocar toda a memória da máquina virtual dentro de uma área reservada da memória RAM, restringindo a quantidade e o tamanho das memórias das máquinas virtuais em execução para um determinado momento;
6. Permitir que parte da memória da máquina virtual em swap aloque um espaço moderado para troca em disco se necessário;
7. Permitir que a memória das máquinas virtuais faça swap em disco se necessário.

O processo de gerenciamento de memória em máquinas virtuais pode afetar a quantidade de informação recuperável da máquina virtual. Algumas tecnologias de virtualização fazem uso de tabelas de paginação enquanto outras não, exceto em caráter temporário, sendo que através de modificações no kernel é possível se garantir acesso limitado do sistema operacional hóspede às tabelas de paginação da memória física. Para isso, uma tabela de paginação é mantida para prover o acesso virtual entre as páginas de memória virtual do SO convidado (virtual) e as páginas subjacentes da máquina física, protegendo os sistemas operacionais que são convidados de dependerem especificamente da memória física, o que permite ao *hypervisor* otimizar o uso de memória.

A virtualização de memória em máquinas virtuais é baseada no mesmo princípio do monitor de máquina virtual (VMM) utilizado para controlar os arquivos de paginação enquanto o sistema operacional mantém uma tabela de endereços de páginas virtuais para cada processo que corresponda aos da página física.

Nas tecnologias de virtualização mais comuns, para aumentar ou diminuir dinamicamente a quantidade de memória alocada às máquinas virtuais, ou um driver de memória é carregado para o sistema operacional hóspede, ou a paginação é implementada a partir da VM em um arquivo de swap de servidor. Dessa forma, quando uma máquina virtual é ligada, um arquivo de swap é criado no mesmo diretório que o arquivo de configuração da máquina virtual, sendo que o controlador de memória faz parte do pacote de ferramentas e drivers da VM, os quais se não

estiverem instalados, fazem com que o SO anfitrião use a sua área de swap em disco para forçar a recuperação da memória.

3.6 Análise de Memória

A alocação de memória física e memória virtual em máquinas virtuais ocorre através da interação entre o sistema operacional hospedeiro e o ambiente virtualizado. A máquina física virtualiza o gerenciamento de memória para o sistema operacional convidado. Como resultado, o acesso direto à memória física real não é permitido pelo sistema operacional convidado. Para isso, o VMM utiliza as tabelas de paginação para mapear a alocação de memória do SO convidado e coordena o mapeamento de memória com a máquina física.

Posto isso, a quantidade de memória RAM alocada individualmente para as máquinas virtuais tem o mínimo de impacto sobre o ambiente, devido à forma que o anfitrião (máquina física) reserva memória para as máquinas virtualizadas, ou seja, mesmo que mais memória física seja alocada para uma máquina virtual a fim de que ela não acesse muitas vezes a memória virtual, não há nada que acarrete no declínio da quantidade de dados recuperáveis a partir do arquivo de swap mesmo com o aumento da quantidade de memória RAM.

A análise da memória de alguns ambientes virtualizados é mais simples que outras análises. A investigação do conteúdo da memória de uma máquina virtual em um ambiente virtualizado, é mais facilmente analisada capturando-se e analisando-se arquivo correspondente à sua memória utilizada, que nada mais é que o arquivo de paginação da máquina virtual, ou seja, é um backup da memória principal do sistema operacional convidado.

Esse arquivo está localizado no sistema de arquivos do host e é criado na inicialização da máquina virtual e para se recuperá-lo é possível pausar a VM e então usar qualquer ferramenta de análise para analisa-lo.

Existem muitas ferramentas disponíveis para fazer as coletas e análises especificadas - desde ferramentas comerciais a ferramentas open-source.

4. Análise Forense Computacional ee Ambientes Virtualizados – Abordagem de *Dead Analysis* (*Post Mortem*)

Tradicionalmente, os peritos computacionais forenses usam máquinas virtuais para criar ambientes isolados para análise de *malwares* e vírus ou para ver o ambiente da mesma maneira que o suspeito, de tal forma que seja possível ao perito iniciar a

imagem ou o disco em um ambiente virtual a fim de se visualizar o sistema numa perspectiva em nível de usuário. Essa metodologia propicia um ambiente de configurações controladas que não modificam o sistema operacional hospedeiro e no qual, após o perito proceder as devidas análises forenses, quaisquer modificações podem ser descartadas. Dessa forma, a máquina original é preservada e pode ser utilizada sem quaisquer efeitos adversos.

Atualmente, em vez de se utilizar ambientes virtualizados para se analisar a máquina de um suspeito, os ambientes virtualizados precisam ser analisados. Como descrito anteriormente, a tecnologia de virtualização é usado em todas as facetas de ambientes corporativos desde o datacenter ao desktop. Além disso, a mobilidade e portabilidade de aplicações permitem maior flexibilidade e facilidade no uso e transporte do seu ambiente de trabalho. Ambientes inteiros podem ser levados em dispositivos portáteis como em uma unidade USB, por exemplo, onde um sistema operacional pode ser fácil e independentemente executado. Assim sendo, com uma mídia removível, o único lugar em que a evidência de um delito digital pode se localizar é na memória de acesso aleatório (RAM), a qual é apagada quando o computador é desligado. Esses ambientes, combinados com a possibilidade de se baixar uma máquina virtual da Internet, mudaram o cenário e o contexto das evidências digitais. Todas essas mudanças tecnológicas trazem novos desafios aos métodos tradicionais de realização de análise forense computacional.

Muitas perícias forenses computacionais ainda são realizadas utilizando-se o método tradicional da criação de uma cópia forense (imagem forense) da máquina do suspeito através de um bloqueador de escrita em disco e depois usar essa imagem para criar um caso em um software de análise forense (como o FTK, por exemplo). Contudo, esse método não permite ao perito ver dentro da máquina virtual. Em vez disso, deve-se procurar por sinais de que um ambiente virtual foi utilizado e, em seguida, montá-lo para se examinar seus arquivos.

Como discutido anteriormente, as máquinas virtuais constituem-se de arquivos no disco rígido, os quais podem ser facilmente copiados, excluídos ou armazenados em locais remotos. As tecnologias de virtualização são capazes de fazer uma imagem instantânea (*snapshot*) de uma máquina virtual, a qual pode ser posteriormente revertida ao seu estado original (momento em que foi copiada). O conceito por trás dos snapshots é análogo à criação de um ponto de restauração - onde e quando são armazenadas todas as informações de configuração do sistema

para posterior restauração caso necessário. Havendo possibilidade de se ter evidências nos mesmos.

A seguir serão abrangidos os principais arquivos de instalação, entradas de registro, artefatos e outros itens que um perito pode encontrar quando se tratar de análise forense computacional de ambientes virtualizados.

4.1 Formatos de Imagens de Discos Virtuais

Formatos virtuais podem ter diferentes localizações de arquivos e cabeçalhos de um ambiente real, quando da análise de ambientes virtualizados. Os formatos de imagens de discos virtuais são os mais variados, sendo que os tipos mais comuns são:

8. Fixa - arquivo de imagem atribuído ao disco fixo com seu mesmo tamanho.
9. Dinâmica - arquivo de imagem que é tão grande quanto os dados que estão sendo escritos em disco, incluindo o tamanho do cabeçalho e do rodapé.
10. Diferenciada - representação em bloco do estado do disco virtual comparado ao real.

Dentre esses três tipos de formatos de discos virtuais mais comuns, a imagem do tipo dinâmica tem a peculiaridade de ser constantemente ajustada e pode crescer até o tamanho alocado, com um limite máximo de 2040 gigabytes.

O rodapé de um arquivo de disco virtual é a parte fundamental da imagem e é espelhado como um cabeçalho antes do arquivo para fins de redundância. Dessa forma, sempre que um bloco de dados é adicionado ao arquivo que monta o disco, o rodapé é movido para o final do arquivo.

Uma imagem de disco diferenciada é uma representação em bloco do estado do disco virtual comparado ao real. Assim sendo, esse tipo de imagem é dependente do disco real para ser totalmente funcional.

A imagem do disco real pode ser fixa, dinâmica ou diferenciada. Como a imagem diferenciada de disco armazena o localizador de arquivo do disco real dentro de si mesma, quando este tipo de disco é aberto por uma máquina virtual, o disco real também é aberto. Se o disco real puder ser um disco diferenciado, pode-se então montar uma cadeia de imagens diferenciadas de discos rígidos onde imagens do tipo fixa ou dinâmica podem ser encontradas. Em assim sendo, os formatos de disco rígido são projetados para armazenar arquivos localizadores do

disco real para diferentes plataformas ao mesmo tempo, a fim de apoiar o movimento de discos rígidos entre plataformas.

Em imagens de disco dinâmicas e diferenciadas, os dados do campo offset do rodapé da imagem apontam para uma estrutura secundária que fornece informações adicionais sobre a imagem de disco. O cabeçalho da imagem dinâmica aparece em um setor limitado do disco (512 bytes).

O primeiro setor de um disco virtual é o MBR (como nos discos reais). A partir dele, as partições no disco virtual podem ser determinadas. Geralmente a primeira entrada é a partição de *boot* (primária). Através das estruturas para o MBR, o setor de inicialização pode ser determinado. Assim sendo, o setor de inicialização é o setor de boot da partição e a cadeia, desde o primeiro setor até o setor de *boot* é consistente e pode ser determinada pelo código baseado na especificação acima.

4.2 Recomendações

Ferramentas de varredura e exploração como sniffers, podem ser muito úteis no processo de análise forense computacional de ambientes virtualizados. Entretanto, seu emprego requer muita atenção, cautela e expertise pericial, uma vez que os resultados obtidos com suas capturas podem necessitar de informações que requeiram análises adicionais, as quais podem ser mal interpretadas, se não forem minunciosamente investigadas e estudadas.

Como os dispositivos estão se tornando cada vez menores e com maior capacidade, eles podem ser facilmente escondidos. Assim sendo, os ambientes físicos devem ser examinados de perto e *in loco*.

Na análise de um dispositivo removível, procedimentos para o bloqueamento de escrita são empregados para se fazer sua imagem forense, mas o perito deve ter cautela e considerar a utilização, pelo drive, de utilitários como o *USB Hacksaw* e que podem comprometer o exame máquina. Além disso, o uso de ferramentas como o *Switchblade*, para coleta de informações, pode afetar a máquina do perito e suas análises.

5. Conclusões

A grande abrangência da atividade forense computacional em diversas áreas que envolvem segurança computacional traz complexidade aos trabalhos a serem realizados na investigação de cada caso. A validade técnica e jurídica das

metodologias para recuperar dados de computadores envolvidos em incidentes de segurança tem se tornado fundamental, pois os procedimentos têm que ser tecnologicamente robustos para garantir que toda a informação útil como prova seja obtida e também de uma forma a ser legalmente aceita de forma a garantir que nada na evidência original seja alterado, adicionado ou excluído.

Os ambientes virtualizados podem fazer da investigação forense uma tarefa difícil, já que a virtualização de hosts, aplicativos e sistemas operacionais tende a deixar as evidências dispersas. Outro problema quando da análise forense computacional de ambientes virtualizados é descobrir onde a informação está ou é armazenada. O perito precisa acompanhar constantemente as dinâmicas melhorias e novas técnicas, as diferenças entre os produtos e quais arquivos são interessantes para coleta e análise.

Referências

1. Galvão RKM. Perícia Forense Computacional. Rio de Janeiro: UNIRIO, 2009.
2. Morrison B. Gestão de Riscos em Ambientes Virtuais. São Paulo: Onicommunications, 2009.
3. Marins CE. Desafios da Informática Forense no Cenário de Cloud Computing. Brasília: ICOFCS, 2009.
4. Melo S. Computação Forense Com Software Livre - Conceitos, Técnicas, Ferramentas e Estudos de Casos. Rio de Janeiro: Alta Books, 2009.
5. Ormandy T. An Empirical Study into the Security Exposure to Hosts of Hostile Virtualized Environments. California: Google Inc., 2009. PMCid:PMC2650420.
6. Barret D. Virtualization and Forensics - A Digital Forensic Investigator's Guide to Virtual Enviroments. 1ª Edição. Burlington: Syngress, 2010.
7. Bawcom A. Virtualization for Security - Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting. 1ª Edição. Burlington: Syngress, 2009.