Uma proposta para automatização do processo de preservação de evidências voláteis em sistemas *in vivo* com ênfase em *hosts Linux*

Osmany Dantas Ribeiro de Arruda[1]
Anderson Aparecido Alves da Silva[2]
Adilson Eduardo Guelfi[3]
Sérgio Takeo Kofuji[4]

Resumo:

O ordenamento jurídico brasileiro define os crimes cibernéticos como próprios ou impróprios. O crime cibernético próprio pode ser simplificadamente definido como aquele onde o bem jurídico tutelado é a informática, por exemplo, no caso de destruição de uma base de dados. Já o crime cibernético impróprio, refere-se ao emprego de recursos informáticos como auxiliares na prática de ilícitos, como o uso das mídias sociais para ataques a honra. Logo, o computador poderá se tornar um local de crime, no qual a abordagem *in vivo* poderá produzir evidências reconhecidamente relevantes, tais como a identificação dos processos em execução e das conexões de rede ativas, dentre outras informações normalmente indisponíveis em análises *post-mortem*.
Palavras-Chave: Crimes cibernéticos; local de crime; *in vivo*; *post-mortem*.

Abstract:

The Brazilian legal system defines cybercrimes as proper or improper. In a simple way, proper cybercrimes can be defined as the one where the legal good protected is the information technology, for example, in case of destruction of a database. Improper cybercrime, however, refers to the use of computer resources as an aid to illicit practices, such as the use of social media to attack honor. Therefore, the computer may turn into a crime scene, where the in vivo approach could produce relevant evidence, such as the identification of running processes and active network connections, among other information not usually available in post-mortem analysis.
Keywords: Cybercrimes; Crime scene; *in vivo*; *post-mortem*.

Introdução

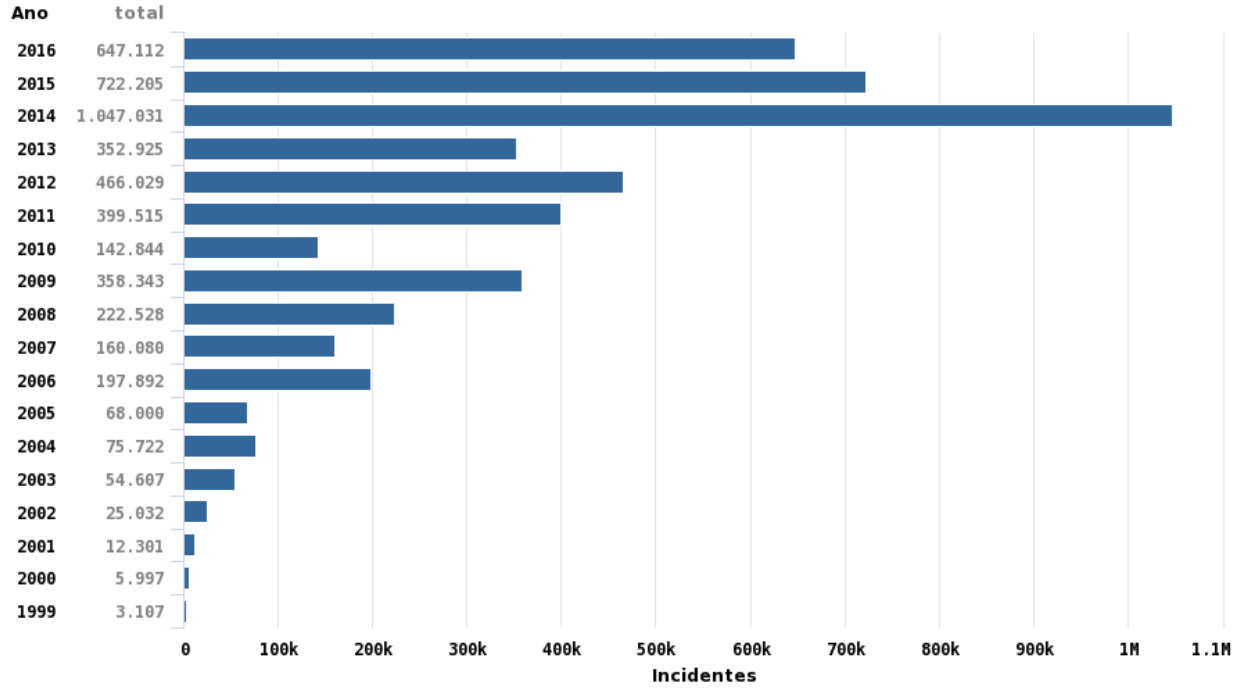
O expressivo crescimento verificado em relação ao uso dos recursos e serviços computacionais ao longo das últimas décadas trouxe consigo novas e deturpadas formas de utilização dos computadores, os quais passaram a ser empregados também como poderosas ferramentas em condutas delituosas, fato que, dentre outras maneiras, pode ser verificado por meio

[1] Professor Mestre na Faculdade de Informática e Administração Paulista - FIAP
[2] Professor Doutor no Instituto de Pesquisas Tecnológicas de São Paulo - IPT
[3] Professor Doutor no Instituto de Pesquisas Tecnológicas de São Paulo - IPT
[4] Professor Doutor na Universidade de São Paulo - USP

da escalada de incidentes de segurança reportados ao CERT.br (Figura 1).

Fatores como a falsa sensação de anonimato proporcionada pelos computadores, aliada a possibilidade de ganhos financeiros sem violência nem qualquer interação física com a vítima, e ainda a notória profusão dos serviços computacionais, certamente podem ajudar a explicar a escalada verificada em relação aos crimes cibernéticos, destacando-se neste contexto as fraudes, que por si só, representam 15,87% dos incidentes reportados ao CERT.br no período de janeiro a dezembro de 2016 (CERT.br, 2017).

Figura 1 – Total de incidentes reportados ao CERT.br por ano



Fonte: CERT.br (2017)

Edmond Locard (1877-1966), cientista forense do início do século XX, postulou um dos princípios fundamentais da ciência forense, conhecido como o Princípio da Troca de Locard (*Locard Exchange Principle*, 1920), o qual, de forma bastante sucinta (HORSWELL, 2004; JR et al., 2012), afirma que todo contato deixa vestígios, e assim sendo, tem-se: de um lado, o autor do delito deixando vestígios de sua passagem no local de crime, e de outro, o autor do delito levando consigo vestígios de sua permanência (ou ações) no local de crime. Por sua vez, Lazaridis, Arampatzis e Pouros (2009) definem a perícia forense computacional digital - a partir daqui também referenciada simplesmente como forense computacional, como a ciência que trabalha com a descoberta, validação e interpretação de evidências digitais encontradas em dispositivos eletrônicos, tendo como principais objetivos a recuperação e preservação destas evidências; o que permite afirmar por analogia com o mundo real, que quando da perpetração de um crime

informático[5], o computador também passa a ser um local de crime, e desta maneira, objeto das práticas forenses pertinentes.

Logo, a forense computacional poderá oferecer relevante contribuição não apenas para esclarecimento de incidentes de segurança da informação, mas também, para fortalecimento das políticas e processos relacionados a esta em ambiente corporativo. Ao responder aos mesmos questionamentos formulados no mundo real (HORSWELL, 2004), a forense computacional busca a apuração da autoria e das circunstâncias que possibilitaram a consumação do ilícito: identificação das credenciais utilizadas (quem) e ações executadas pelo autor no sistema alvo (o que), determinação da cronologia dos eventos (quando), da origem (onde) e da motivação (por que) do incidente, dentre outros pontos. Jr et al. (2012) definem a evidência digital como toda e qualquer informação digital capaz de determinar a ocorrência de uma intrusão, ou que forneça alguma ligação entre o delito e as vítimas ou entre o delito e o atacante. Em sistemas in vivo, há que se ter sempre em mente a volatilidade característica deste tipo de evidência, sendo razoável, portanto, assumir que sua preservação e recuperação serão mais eficientes quando devidamente assistidas por processo específico e adequado à condução dos trabalhos periciais (FARMER; VENEMA, 2011).

Objetivo

Este trabalho tem como objetivo geral a proposição das bases de um processo para preservação da evidência digital de alta volatilidade para fins forenses e resposta a incidentes, aqui restrito ao conteúdo da memória volátil (RAM) em sistemas computacionais Linux *in vivo*; tendo ainda como objetivo específico, a produção de ferramenta básica em *software* (*shell script*), a ser utilizada como instrumento de referência pelo *first responder* para automatização das tarefas repetitivas do referido processo.

Referencial teórico e modelo de referência para e-discovery

De acordo com Farmer e Venema (2011), o PRINCÍPIO DA INCERTEZA DE HEISENBERG é diretamente aplicável à coleta de dados em sistemas computacionais, e em decorrência disto torna-se não apenas difícil - mas essencialmente impossível, a coleta de todas as informações em um sistema computacional. Entretanto, isto não pode ser atribuído predominantemente ao Princípio da Incerteza de Heisenberg, mas sim, ao fato de computadores

[5] Definição jurídica disponível em <http://www.egov.ufsc.br/portal/conteudo/crimes-inform%C3%A1ticos-delitos-virtuais-no-direito-brasileiro>. 2015. Acesso em: 17 ago. 2017.

não serem definidos por seu estado em um determinado momento, mas em relação a uma série contínua; e desta forma, memória, processos e arquivos podem ser entidades tão dinâmicas que o registro preciso e sincronizado de suas atividades não é possível sem perturbar profundamente a operação de um sistema computacional típico.

Ainda segundo com Farmer e Venema (2011) a coleta de dados em um sistema computacional deve ocorrer de forma ordenada a fim de que seja garantida a preservação da evidência digital, uma vez que, quanto mais volátil, mais suscetível a perdas e modificações ela se torna. Esta ordem tem como base a expectativa de vida dos dados (da evidência), sendo denominada ORDEM de VOLATILIDADE (Quadro 1).

Quadro 1 – Ordem de Volatilidade

Tipos de dados	Tempo de Vida
Registradores, memória periféricos, caches, etc.	nanossegundos
Memória principal	10 nanossegundos
Estado da rede	Milissegundos
Processos em execução	Segundos
Disco	Minutos
Disquetes, mídias de backup	Anos
CD ROMs, impressões	Dezenas de anos

Fonte: Farmer e Venema (2011)

Hausknecht, Foit e Buric (2015) afirmam que dados voláteis, especialmente os residentes na memória RAM, não poderão ser adequadamente preservados caso o sistema sob investigação venha a ser desligado, enfatizando ainda, que grande parte dos dados e informações que trafegam pelo sistema, podem nunca ser registrados em disco, residindo unicamente na memória RAM.

Ainda segundo estes autores, algumas das informações mais relevantes possivelmente encontradas na análise da memória RAM recaem sobre processos, arquivos abertos, tráfego da rede, senhas e chaves criptográficas, dentre outros. Em última análise é possível afirmar, portanto, que a preservação da evidência digital pode ser concretizada na forma do *dump* e gravação do conteúdo da memória RAM.

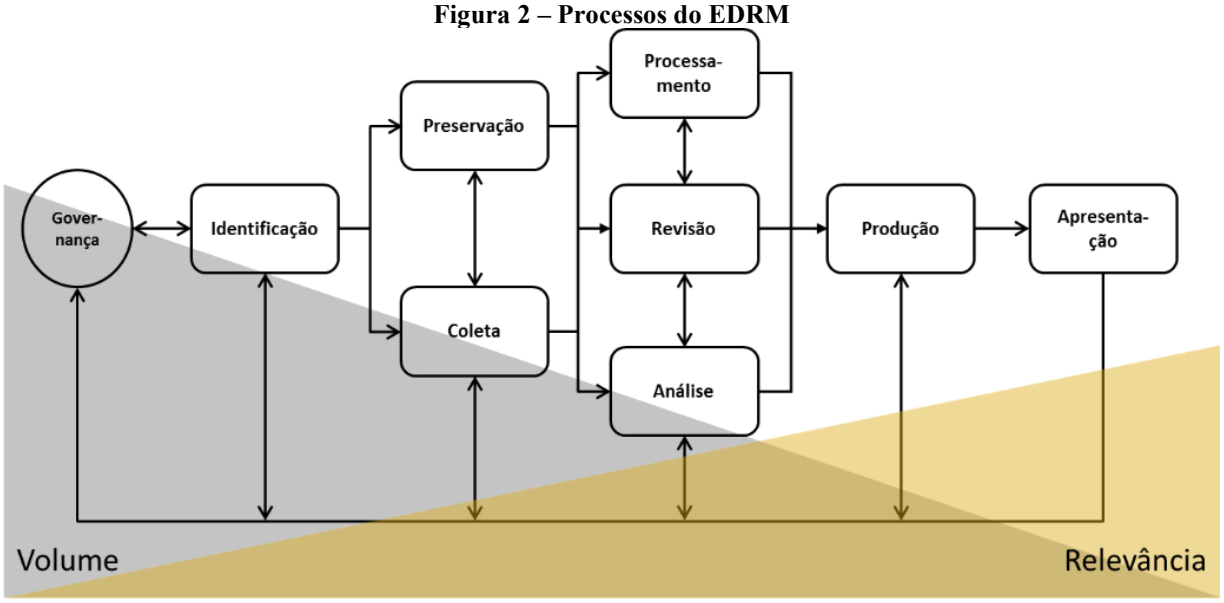
Todavia, o dinamismo e a volatilidade, duas das principais características deste tipo de memória, representam expressivos desafios à preservação da evidência, na medida em que à luz do Princípio da Incerteza de Heisenberg (1927), sabe-se ser impossível a obtenção da totalidade dos dados residentes na RAM em razão dos diferentes estados que as múltiplas regiões da memória poderão assumir ao longo do processo; tornando imprescindível, portanto, a rigorosa observância da Ordem de Volatilidade (FARMER; VENEMA, 2011) a fim de maximizar o volume de dados preservados para coleta.

O LiME é um *loadable kernel module* (LKM), um módulo que possibilita o *dump* do conteúdo da memória volátil (RAM) em sistemas *Linux* e derivados, como o *Android*, tendo também como compromisso, minimizar a interação entre o usuário e os processos executados em *kernel space* ao longo do processo de extração do conteúdo da RAM, fato que aliado a possibilidade de transmissão do *dump* via rede para armazenamento remoto, pode torná-lo menos intrusivo ao sistema investigado, contribuindo para otimização do processo de preservação da evidência digital (JONES; ETZKORN , 2016).

Ng (2007) afirma que a coleta de evidências sem metodologia definida, testada e validada representa considerável risco de contaminação da evidência, sendo complementado por Kornblum (2002), o qual enfatiza que frequentemente a contaminação da evidência digital é fruto das boas intenções do *first responder*, e resultante da interação desmedida deste com o objeto questionado, em sua busca por evidências antes que a devida preservação do ambiente tenha sido garantida.

A necessidade de um modelo de referência profuso, e que gozasse de efetivo reconhecimento pelo mercado, levaram à adoção do *ELECTRONIC DISCOVERY REFERENCE MODEL* (EDRM) como referência para desenvolvimento deste trabalho, o qual representa uma visão conceitual do processo de *e-discovery* sendo composto por nove processos interligados, porém, independentes entre si (Figura 2).

Figura 2 – Processos do EDRM



Fonte: Adaptado de EDRM.net pelos próprios autores.

Objetivamente descrevendo-se as partes do modelo de maior relevância para este trabalho, tem-se no segundo estágio, o processo de IDENTIFICAÇÃO, responsável pela adequada

identificação das potenciais fontes de informações relevantes, representadas especialmente por pessoas, unidades de negócio, sistemas computacionais, e até arquivos em papéis – dentre outras; cabendo ressaltar ainda, que nesta fase também acontece a identificação positiva do objeto questionado, para registro na CADEIA de CUSTÓDIA.

O terceiro estágio do modelo é constituído por dois diferentes processos: o de PRESERVAÇÃO - responsável por salvaguardar o ambiente e garantir que a informação eletronicamente armazenada (IEA) não seja destruída nem indevidamente alterada; e o de COLETA, cuja função é reunir a IEA para posterior utilização pelos processos de *e-discovery*.

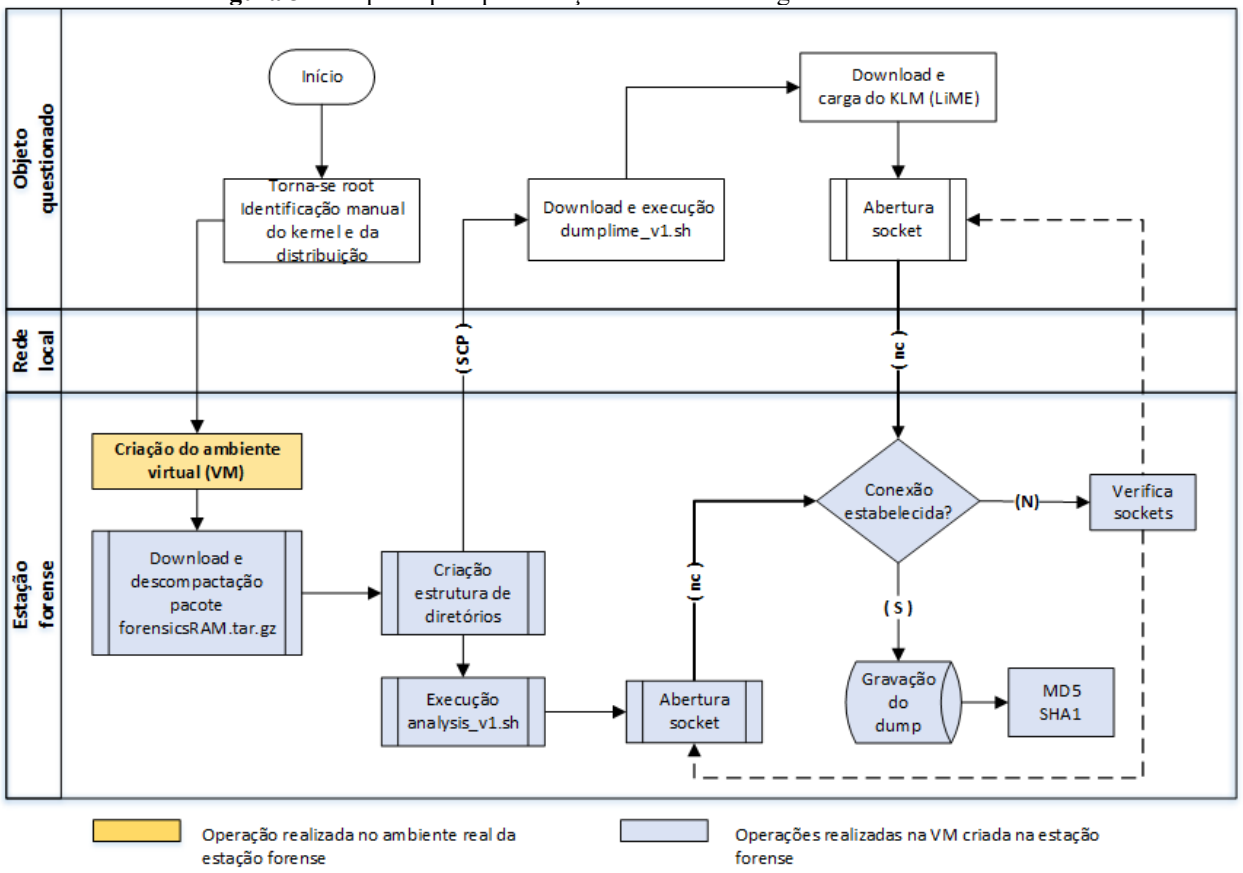
O quarto estágio conta com três processos: o PROCESSAMENTO, responsável pelo refinamento inicial da IEA, isolando as informações aderentes ao contexto da investigação naquele momento - assim reduzindo o volume e aumentando a relevância da informação a ser repassada ao processo subsequente, de REVISÂO, no qual o investigador busca melhor entendimento e classificação do conteúdo das informações obtidas, bem como, sua organização em subconjuntos adequados.

Finaliza este estágio, o processo de ANÁLISE, o qual tem como objetivo o exame do conteúdo e do contexto da IEA previamente tratada, a fim de apurar fatos, construir cronologias e oferecer subsídios para resposta à quesitação proposta.

Visão geral do processo proposto para preservação da evidência digital in vivo

Tratando-se de sistema *in vivo*, os procedimentos referentes à preservação da evidência digital tornam-se um tanto limitados em termos práticos, basicamente, recaindo sobre a minimização da interação do investigador com o ambiente. A coleta das evidências depende da produção do LKM – no caso, o LiME, a ser carregado para a memória. Todavia, da Ordem de Volatilidade (FARMER; VENEMA, 2011) e do Princípio da Troca de Locard (1920) vem a impossibilidade de produção deste no próprio objeto questionado, dada a contaminação e potencial perda de evidências resultantes, propondo-se então, o processo representado na Figura 3 para mitigação de tais efeitos e automatização das tarefas repetitivas para preservação da evidência digital.

Figura 3 – Proposta para preservação da evidência digital de alta volatilidade



Fonte: Elaborado pelos autores.

Da Figura 3 observa-se que o processo proposto para preservação da evidência digital em sistemas *in vivo* é iniciado no objeto questionado, com a identificação da distribuição e do *kernel* em execução, procedendo-se então, a virtualização de réplica deste ambiente na estação forense, onde o LKM será produzido e posteriormente baixado e carregado para a memória do objeto questionado. Ao ser carregado o LKM criará um *socket* no objeto questionado, o qual ao ser conectado a outro *socket* criado na estação forense, dará início ao *dump* da RAM.

Experimento

O experimento foi conduzido com base em três cenários distintos. No primeiro, o processo para preservação da evidência digital foi integralmente aplicado, buscando-se maximizar a preservação limitando a interação do investigador com o ambiente do objeto questionado, essencialmente, por meio da automatização das tarefas repetitivas do processo de preservação com auxílio de *shell scripts*[6], sendo o LKM produzido e armazenado na estação forense, bem como, o

[6] Os scripts criados são ferramentas básicas, porém funcionais em todos os aspectos estritamente relacionados ao *dump* da RAM, podendo ser baixados, a partir de https://mega.nz/#F!EwojXaKD, key: !Lew_3VS6JlhI3oE_2DIDNw, onde é disponibilizada também a integra do trabalho que originou este artigo.

dump da RAM.

No segundo cenário, foi promovida maior interação do investigador com o ambiente do objeto questionado, ao se conduzir manualmente as tarefas repetitivas do processo de preservação, como a carga do módulo, a criação dos *sockets* e a própria execução do *dump*. A produção do LKM e o armazenamento do *dump* continuaram sendo realizados na estação forense. No terceiro cenário, todas as tarefas referentes ao procedimento pericial foram desenvolvidas de forma totalmente manual e diretamente no objeto questionado, incluindo o *download* e instalação dos pacotes adicionais necessários à produção do módulo, *download* e descompactação do pacote do LiME (*master.zip*) e ainda, a compilação e carga do módulo (LiME) dentre outras, sendo mantido apenas o armazenamento do *dump* na estação forense.

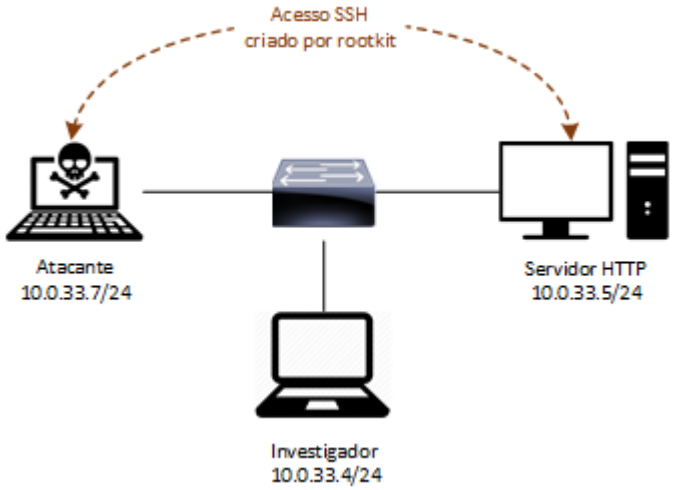
Em cada um destes cenários, uma distribuição Linux diferente foi utilizada para a virtualização do objeto questionado, o qual contava ainda, com quatro processos de controle. Cada *host* virtual tinha então este estado inicial preservado por meio de *snapshot* permitindo, assim, sua restauração sempre que necessário.

Estes processos de controle consistiam de: (a) um terminal executando a ferramenta *iptraf* para monitoramento do tráfego da rede, (b) um terminal executando a ferramenta *nmon* para monitoramento do uso de memória real e virtual, (c) um terminal executando a ferramenta *nmon* para monitoramento em tempo real dos processos em execução, mais uma conexão SSH originada por outro *host* Linux simulando um acesso remoto não autorizado ao objeto questionado (servidor HTTP).

Com base na Ordem de Volatilidade e nas obras referenciadas, as seguintes evidências foram pesquisadas nos *dumps* produzidos nos diferentes cenários: (a) Conteúdo da RAM, (b) Conexões de rede, (c) Processos e (d) Comandos executados pelo investigador.

A Figura 4 ilustra a topologia de referência implementada em todos os cenários do experimento.

Figura 4 – Topologia de referência do experimento



Fonte: Elaborado pelos autores.

O Quadro 2 detalha as configurações dos *hosts* utilizados nos diferentes cenários, utilizando-se o *VirtualBox* 5.2.6 como *hypervisor* em todos estes, cabendo salientar a não instalação do adicional de convidados nas VMs utilizadas como objeto questionado, dadas as modificações imputadas ao *kernel* original, tendo-se ainda, observado prejuízo aos perfis criados para uso do *Volatility.*

Quadro 2 – Configurações dos *hosts* virtuais (VMs) utilizados

Host	Distribuição	Kernel	RAM	vHD	vCPU
Atacante	*Debian Jessie* 8.1	3.16.0-4-amd64	1GB	15GB	1
Investigador	*Debian Jessie* 8.1	3.16.0-4-amd64		15GB	
Objeto questionado I (Servidor HTTP)	*Point Linux* 3.2 (*Agni*)	3.16.0-4-amd64	1GB	8GB	
Objeto questionado II	*Debian* 8.1 (*Jessie*)	3.16.0-4-amd64		15GB	
Objeto questionado III	*Mint LMDE2* (*Betsy*)	3.16.0-4-amd64		10GB	

Fonte: Elaborado pelos autores.

Resultados

Todas as evidências originalmente produzidas pelo experimento estão disponíveis em https://mega.nz/#F!EwojXaKD, key: !Lew_3VS6JlhI3oE_2DIDNw, tendo sido coletadas por intermédio do LiME e processadas com auxílio do Volatility.

Novas conexões (*sockets*) criados

A Tabela 1 apresenta a relação entre as novas conexões criadas especificamente pelo processo proposto para preservação do conteúdo da RAM e a quantidade total de conexões ativas quando do *dump* desta, sendo razoável assumir-se como aceitável o grau de contaminação apurado (>1%).

Tabela 1 - Contaminação do conteúdo da RAM por novas conexões

Cenário	Quantidade total de conexões verificadas na RAM	Quantidade de novas conexões estabelecidas pelo processo	Grau de contaminação	
			(%)	Avaliação
1	471	3	>1%	Aceitável
2		3		
3		2		

Fonte: Elaborado pelos autores.

Novos módulos carregados para a RAM

Este tópico foi abordado sob duas perspectivas distintas e complementares a fim de produzir resultados mais confiáveis. A Tabela 2 relaciona o espaço alocado em memória pela carga do LiME com a quantidade total de memória RAM disponível.

Tabela 2 - Utilização de espaço de endereçamento da RAM pelo LiME

Cenário	Tamanho total do espaço de endereçamento da RAM	Quantidade de memória utilizada pelo LiME	Grau de contaminação	
			(%)	Avaliação
1	1GB	≈18,2KB	>1%	aceitável
2				
3				

Fonte: Elaborado pelos autores.

A Tabela 3 avalia quantitativamente o impacto da carga do novo módulo (LiME) para a RAM tomando como referência a quantidade de módulos já residentes nesta, quando da produção do *dump*.

Tabela 3 - Utilização de espaço de endereçamento da RAM pelo LiME

Cenário	Quantidade total de módulos carregados na RAM	Quantidade de novos módulos carregados pelo processo	Grau de contaminação	
			(%)	Avaliação
1	59	1	≈1,7%	Aceitável
2				
3				

Fonte: Elaborado pelos autores.

Os resultados apontados em ambos os casos (>2%) sugere que também em relação a estes quesitos, o grau de contaminação do conteúdo da RAM promovido pelo processo de preservação proposto é desprezível.

Comandos executados

Analogamente aos quesitos 6.1 e 6.2, também a quantidade de comandos executados – direta ou indiretamente ligados ao processo proposto para preservação da evidência digital se mostrou reduzido em relação às atividades normais de um sistema em produção evidenciando, entretanto, que a contaminação do conteúdo da RAM decorrente da interação do investigador com o objeto questionado é mais pronunciada no cenário 3 dada a execução das tarefas secundárias necessárias ao processo investigativo, tais como: atualização de repositórios, instalação de pacotes adicionais e a preparação do módulo, dentre outras (Tabela 4).

Ainda em relação ao referido cenário, há que se considerar adicionalmente, a contaminação do disco rígido do objeto questionado decorrente da execução destas tarefas, potencialmente comprometendo desta forma, as evidências neste armazenadas e, portanto, potencialmente prejudicando uma posterior análise *post-mortem*.

Frente a isto considera-se, em princípio, o processo proposto como NÃO DIRETAMENTE APLICÁVEL ao contexto do cenário 3, cabendo ao investigador avaliar a melhor forma a proceder.

Entretanto, da análise dos dados da Tabela 4, é possível observar que os resultados obtidos em relação aos cenários 1 e 2 indicam que o grau de contaminação da RAM - resultante estritamente da execução manual dos procedimentos investigativos, é semelhante ao obtido quando da execução automatizada, sugerindo assim, recaírem as vantagens do uso das ferramentas (*scripts*) criadas para preservação do conteúdo da RAM em sistemas com baixa utilização, sobre o aumento da eficiência, melhor reprodutibilidade do processo e prevenção de excessos na interação do *first responder* com o objeto questionado, especialmente, neste último caso, quando da condução do processo em condições adversas, a exemplo da pressão comumente exercida sobre o investigador em ambientes corporativos para que o sistema afetado retorne a produção.

Tabela 4 - Utilização de espaço de endereçamento da RAM pelo LiME

Cenário	Quantidade total de comandos apurados na RAM	Quantidade de comandos efetivamente relacionados ao processo	Grau de contaminação	
			(%)	Avaliação
1	15	5	Não se aplica	Aceitável
2	11	5		Aceitável
3	19	10		Inaceitável

Fonte: Elaborado pelos autores.

Deve ser ressaltado ainda, que antes do início dos procedimentos executados em cada cenário estudado, o ambiente do objeto questionado (VM) era sempre restaurado ao mesmo estado inicial de referência, e assim sendo, os históricos dos comandos anteriormente executados também eram reinicializados.

Daí a pequena amostragem de comandos verificada e a razão da abordagem quantitativa ser considerada como não aplicável ao contexto. Considerando-se, entretanto, a tendência de redução na relação entre a quantidade de comandos executados efetivamente relacionados ao processo investigativo e a quantidade de comandos normalmente executados em sistemas em produção, considera-se como aceitável a aplicabilidade do processo proposto aos cenários 1 e 2.

Novos processos criados

Dos dados apresentados pela Tabela 5, é possível observar que independentemente do cenário abordado, os processos em execução na RAM - estritamente relacionados aos procedimentos executados para preservação da evidência digital, também representam reduzida parcela do universo apurado, sugerindo em função disto, um impacto discreto sobre o conteúdo armazenado na memória volátil.

Tabela 5 - Relação entre a quantidade de processos existentes na RAM

Cenário	Quantidade total de processos em execução na RAM	Quantidade de processos efetivamente relacionados ao *dump*	Grau de contaminação	
			(%)	Avaliação
1	142	8	≈5,6	Aceitável
2	140		≈5,7	
3	140		≈5,7	

Fonte: Elaborado pelos autores.

Vale reforçar, entretanto, que dada a dinâmica do conteúdo RAM, a quantidade de processos alheios aos criados pelos procedimentos para sua preservação, pode variar consideravelmente durante de operação do sistema (Princípio da Incerteza de Heisenberg).

Assim sendo, a fim de se obter *baseline* consistente para avaliação do impacto destes processos sobre o conteúdo da RAM, os procedimentos periciais foram executados em máquinas virtuais (objeto questionado) com instalação básica, as quais – a exemplo do quesito 6.3, eram sempre restauradas aos respectivos estados iniciais de referência antes do início dos testes em cada cenário, permitindo desta maneira, observar com fidelidade a proporção entre a quantidade de processos criados pelo *dump* (preservação) e a quantidade de processos nativos do sistema.

Entretanto, também neste tópico, apenas a relação quantitativa entre estes não é suficiente para uma avaliação adequada, sendo, portanto, considerada também a proporção entre a quantidade de memória física total[7] disponível no objeto questionado e a quantidade alocada para uso pelo processo de preservação (Tabela 6).

Tabela 6 - Relação de uso da RAM pelos processos investigativos

Cenário	Quantidade total de memória física disponível (RAM)	Quantidade total de memória utilizada pelo processo investigativo[8]	Grau de contaminação	
			(%)	Avaliação
1	1GiB	45KiB[9]	>1	Aceitável
2				
3				

Fonte: Elaborado pelos autores.

[7] Considera-se a quantidade total de memória física disponível no sistema com base no fato de que evidências eventualmente existentes no espaço de endereçamento alocado para uso pelos processos investigativos poderão vir a ser sobrescritas por estes.

[8] Válido para os três cenários, uma vez que os procedimentos são os mesmos, mudando-se apenas a abordagem.

[9] Somatória da parcela de memória compartilhada (SHR) e da parcela da memória utilizada (RES) pelos procedimentos investigativos.

Da Tabela 6 é possível concluir que também o consumo de memória estritamente relacionado ao processo investigativo é consideravelmente reduzido, sugerindo assim, contaminação bastante discreta do conteúdo armazenado na RAM.

Conclusão

Dos resultados apurados, considera-se terem as bases propostas ao processo para preservação da evidência digital em sistema *in vivo* se mostrado adequadas e efetivamente aplicáveis.

A automatização unicamente das tarefas repetitivas do processo, por meio de ferramentas simples escritas em *shell script* tornou-o mais eficiente e facilmente reprodutível, diminuindo a interação do investigador com o ambiente do objeto questionado, entretanto, ainda mantendo com ele o controle dos procedimentos e a tomada das decisões necessárias, desta forma, impedindo que detalhes do contexto investigativo viessem a ser perdidos.

A concepção do processo, bem como a definição dos parâmetros a serem coletados durante o experimento foram direcionados, essencialmente, com base na ORDEM DE VOLATILIDADE, PRINCÍPIO DA INCERTEZA DE HEISENBERG e PRINCÍPIO DA TROCA DE LOCARD, cabendo salientar que, embora alguns resultados obtidos possam sugerir que quanto maior a disponibilidade de memória RAM no sistema analisado, inversamente proporcional será o grau de contaminação de seu conteúdo, tal hipótese deve ser avaliada com o devido cuidado pelo investigador, uma vez que sob o ponto de vista forense, algumas informações eventualmente sobrescritas pelo processo talvez viessem a se mostrar mais relevantes à investigação do que a relação meramente quantitativa entre os parâmetros avaliados.

Dentre outros pontos que, embora tangenciais aos objetivos deste trabalho, mostraram considerável relevância ao processo investigativo como um todo, destacam-se: (a) a confirmação de que a produção e utilização dos módulos carregáveis pelo *kernel* (LKM) estão relacionadas ao *kernel* em execução no sistema sob investigação e não propriamente a distribuição adotada, (b) a preocupação em relação ao local de armazenamento do *dump* afim de garantir-se a preservação da evidência ao longo de todo o processo investigativo (*in vivo* e *post-mortem*), (c) deve ser observado que apesar de neste trabalho o processo proposto haver sido implementado e conduzido totalmente em ambiente virtual, não há qualquer impedimento em relação a sua implementação em ambiente real, sendo necessário apenas, que o investigador proceda às adaptações necessárias ao novo contexto, observando as premissas que delinearam o processo, discutidas ao longo deste trabalho.

Referências

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTE DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.br. **Incidentes Reportados ao CERT.br** - Janeiro a Dezembro de 2016. Disponível em <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em: 09 set. 2017.

CHAN, E.M. **A FRAMEWORK FOR LIVE FORENSICS** 2011. 122f. Dissertation - University of Illinois at Urbana-Champaign, Urbana, Illinois, 2011.

EDRM Duke Law. **Electronic Discovery/E-Discovery.** 2017a. Disponível em <http://www.edrm.net/glossary/electronic-discovery-e-discovery/>. Acesso em: 16 mai. 2017.

EDRM Duke Law. **EDRM Model.** 2017b. Disponível em <http://www.edrm.net/frameworks-and-standards/edrm-model/>. Acesso em: 16 mai. 2017.

FARMER, D.; VENEMA, W. **Perícia Forense Computacional – Teoria e Prática Aplicada** 4. Reimpressão, 2011 São Paulo: Pearson Prentice Hall, 2007. 190p.

HAUSKNECHT, K.; FOIT, D.; BURIC, J. **RAM data significance in digital forensics**. In: 38th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2015. Opatija, Croatia, May 2015, p. 1372-1375.

HORSWELL, J. **The Practice Of Crime Scene Investigation**. New York:CRC Press, 2004. 418p.

JONES, J.; ETZKORN, L. **Analysis of Digital Forensics Live System Acquisition Methods to Achieve Optimal Evidence Preservation.** IEEE SoutheastCon

JR, A.P.C. et al. **Forense Computacional em Memória Principal**. 2012. Disponível em <http://www.mp.go.gov.br/portalweb/hp/1/docs/foren-comp-ram.pdf>. Acesso em: 22 mar. 2018.

KORNBLUM, J. **Preservation of Fragile Digital Evidence by First Responders** Digital Forensics Research Workshop, v.8, p.1-11, Aug. 2002.

LAZARIDIS, I.; ARAMPATZIS, T. POUROS, S. **Evaluation of Digital Forensics Tools on Data Recovery and Analysis**. Proceedings of the Third International Conference on Weblogs and Social Media, Thessaloniki, p.67-71, May 2009.

NG, R. **Forense Computacional Corporativa – Motivadores, Planejamento e Custo, Metodologia**. Rio de Janeiro: Brasport, 2007. 180p.

SILBERSCHATS, A.; GALVIN, P.B.; GAGNE, G. **Operating System Concepts.** 9.ed. USA: John Wiley & Sons, Inc, 2012. 976p.

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO – GTA-UFRJ **Princípio da Incerteza de Heisenberg.** Disponível em: <https://www.gta.ufrj.br/grad/07_1/quantica/PrincpiodaIncertezadeHeisenberg.html>. Acesso em: 11 abr. 2007.