

Hamilton Fonte II

# **Coletando dados de memória de uma máquina em nuvem para análise forense**

**São Paulo, Brasil**

**2016, v-0.1**

Hamilton Fonte II

# **Coletando dados de memória de uma máquina em nuvem para análise forense**

Projeto de pesquisa para a disciplina Metodologia de Pesquisa Científica em Engenharia de Computação.

Universidade de São Paulo – USP

Escola Politécnica - Engenharia de Computação

Programa de Pós Graduação em Engenharia Elétrica - Mestrado

Orientador: Marcos Antonio Simplício Jr

São Paulo, Brasil

2016, v-0.1

# Sumário

	<b>Sumário</b> . . . . .	<b>2</b>
<b>1</b>	<b>INTRODUÇÃO</b> . . . . .	<b>3</b>
<b>2</b>	<b>JUSTIFICATIVA</b> . . . . .	<b>4</b>
<b>3</b>	<b>OBJETIVOS</b> . . . . .	<b>5</b>
<b>4</b>	<b>MÉTODOS</b> . . . . .	<b>6</b>
<b>5</b>	<b>REVISÃO BIBLIOGRÁFICA</b> . . . . .	<b>7</b>
<b>6</b>	<b>ANÁLISE DOS RESULTADOS</b> . . . . .	<b>14</b>
	<b>Referências</b> . . . . .	<b>15</b>

# 1 Introdução

Aqui vai a introdução

## 2 Justificativa

Aqui vai a justificativa

## 3 Objetivos

Aqui vão os objetivos

## 4 Métodos

Aqui vão os métodos

## 5 Revisão Bibliográfica

- **Digital forensics framework for a cloud environment (GEORGE; VENTER; THOMAS, 2012)** : Arcabouço para coleta de dados de máquinas virtuais. Possui duas formas de acionamento, a manual e a automática, integrada com algum sistema de detecção de ameaça. Quando acionado, escuta a rede, determina qual máquina é objeto de investigação, coleta informações de log e tráfego de rede e associa ao usuário da respectiva máquina. Propõe o armazenamento das evidências em local fora da nuvem para escapar de problemas de jurisdição e multi-inquilino mas tem inteligência para usar a própria nuvem como armazenamento caso o espaço fora acabe.

A proposta dá a entender que é aplicável apenas a um sistema virtual estático, onde o número e organização das máquinas é constante. De informação volátil coleta apenas tráfego de rede, não coleta memória. Com a forma de acionamento descrito ele não consegue descrever, com as evidências, como era o sistema antes do ataque. Apesar de armazenar a evidência fora da nuvem, não dá detalhes de como garante que a evidência não foi alterada ou destruída no transporte até o local de armazenamento nem como controla o acesso a evidência.

Quando comparado a este trabalho, a presente proposta tem por vantagens a utilização de container para associar a evidência a sua origem tornando o processo independente de máquina e permitindo que seja repetido mesmo se a máquina de onde se originaram os dados não existir mais. Com a implementação de uma janela de x dias de coleta antes da detecção do ataque é possível descrever, através de evidência, como era o sistema antes do mesmo. Com isso a solução apresentada consegue evidências em um cenário de infra-estrutura dinâmica. São tomadas precauções para garantir que os dados não foram alterados ou destruídos no transporte via TLS os para um local fora da nuvem e o acesso a mesma é controlado.

- **Evidence and cloud computing the virtual machine introspection approach (POISEL; MALZER; TJOA, 2013)** : Descreve um método de coleta de informações de máquinas em nuvem através da técnica de introspecção em máquina virtual, onde se acessa os dados das máquinas virtuais através do hypervisor. Propõe que o processo seja disparado automaticamente integrado a um sistema de detecção de ameaça mas também suporta acionamento manual.

A técnica descrita cobre apenas o processo de coleta de informações, não explica onde ou como elas serão armazenadas. No que tange as informações de memória,



como os endereços de memória são os do host, estes precisam ser traduzidos para que a análise forense seja feita. Segundo a comunidade, tal estratégia é imune a técnicas anti-forenses empregadas por usuários maliciosos pois está localizada fora da máquina virtual. Como a abordagem não tem conhecimento do que está rodando dentro da máquina precisa de uma cópia bit a bit da evidência. Embora pareça possível, não descreve como lida com o cenário onde uma máquina é despejada do pool e os recursos liberados.

Quando comparado a este trabalho, a presente proposta tem por vantagens ser um arcabouço para coleta e armazenamento de evidências. Usa-se uma estratégia diferente pois coleta-se a memória diretamente de dentro da máquina virtual onde se evita o problema do gap semântico próprio das soluções por introspecção. Como não precisa realizar tradução de endereços, a presente proposta consegue realizar uma coleta onde os dados já são úteis para análise e pode direcionar a mesma pois tem o conhecimento do que está rodando na máquina. De acordo com a comunidade é mais suscetível a técnicas anti-forenses.

- **Design and implementation of FROST: FoRensic tools for Open STack (DYKSTRA; SHERMAN, 2013)** : Arcabouço para coleta de dados de máquinas virtuais através da API do hypervisor. Isola a máquina virtual afetada do pool original para realização da coleta. Precisa ser acionado quando uma ameaça é detectada. É o mais bem acabado arcabouço de todas as propostas encontradas até agora mas ao detalhar o processo de armazenamento não explica como garante que a evidência não será destruída ou alterada no transporte até o armazenamento nem como controla o acesso a evidência. Por estar integrado ao Open Stack o arcabouço depende de cooperação do provedor de serviços de nuvem onde ele está rodando, isso é considerado problemático pela comunidade pois a prioridade do mesmo é manter o serviço funcionando e não coletar evidências forenses. Como está na mesma camada do hypervisor não conhece o que está rodando dentro da máquina. Depende da existência da máquina virtual para realização da coleta.

Quando comparado a este trabalho, a presente proposta tem por vantagens a utilização de container para associar a evidência a sua origem tornando o processo independente de máquina e permitindo que seja repetido mesmo se a máquina de onde originaram os dados não existir mais. Com a implementação de uma janela de x dias de coleta antes da detecção do ataque é possível descrever, através da evidência, como era o sistema antes do mesmo. Não depende de cooperação do provedor do serviço de nuvem. A presente proposta também consegue realizar uma coleta onde os dados já são úteis para análise e pode direcionar a mesma pois tem o conhecimento do que está rodando na máquina.

- **Automated Forensic Data Acquisition in the Cloud (REICHERT; RICHARDS; YOSHIGOE, 2015)** : Propõe um modelo que tira instantâneos de máquinas virtuais atrelado a algum mecanismo de detecção de ameaça baseado no hypervisor. Usa o Google Rapid Response para salvar as informações coletadas fora da nuvem de forma a driblar os problemas de multi-jurisdição e multi-inquilino. Descreve satisfatoriamente como evita que a evidência seja alterada ou destruída no transporte até o armazenamento e como controla o acesso a evidência.

O modelo proposto só começa a coletar evidência após a detecção da ameaça e toma um instantâneo da máquina toda o que já foi julgado pela comunidade como um processo custoso em termos de espaço em disco e piora o problema do volume de dados a ser analisado. Pessoalmente acho arriscado depender de instantâneos pois caso precise, repetir o processo de coleta pode não ser possível. Um exemplo é editar um disco virtual que estava atrelado a uma máquina virtual da qual se gerou os instantâneos, tal ação pode levar a perda de dados.

Quando comparado a este trabalho, a presente proposta tem por vantagens coletar apenas as informações de memória e usar a janela de coleta de x dias antes do ataque para manter sob controle a quantidade de informação que precisa ser analisada. Propondo a utilização de container para associar a evidência a sua origem, tornamos o processo independente de máquina.

- **A log based approach to make digital forensics easier on cloud computing (SANG, 2013)** : Método sugere salvar a informação coletada fora da nuvem de modo a driblar os problemas de multi-inquilinato e multi-jurisdição, usa um mecanismo de hash para garantir a autenticidade e integridade da informação mas não dá detalhes da implementação e não descreve como controla o acesso a evidência armazenada. Segundo o próprio autor, o método não funciona em IaaS. Precisa da cooperação do provedor de nuvem pois depende das informações que este último decidiu adicionar ao log. O método não é aplicável a coleta de informações de memória.

A proposta não coleta dados de memória por decisão do autor, esta proposta entrou na lista pela abordagem baseada em log. Neste quesito, a presente proposta é a melhor pois garante que a evidência não foi alterada ou destruída no transporte e o acesso a mesma é controlado. No âmbito da informação coletada, a presente proposta não depende das decisões do provedor de nuvem sobre o que guardar no log para conseguir a evidência.

- **Volatile memory acquisition using backup for forensic investigation (DEZ-FOULI et al., 2012)** : Técnica desenvolvida para dispositivos móveis que sugere a utilização do próprio como repositório das evidências coletadas da memória. Para manter a utilização de espaço ao mínimo sugere manter apenas o último estado conhecido da memória.

É uma técnica interessante do ponto de vista de estratégia de armazenamento quando guarda apenas o último estado da memória. Essa abordagem porém perde a informação do momento do ataque e não consegue descrever o sistema antes do mesmo. Do resto da proposta não é aplicável para este projeto pois, armazenando a evidência na máquina a mesma seria perdida quando a máquina fosse despejada do pool e seus recursos liberados. A cadeia de custódia não é abordada na proposta.

- **Narrowing the semantic gap in virtual machine introspection (DOLAN-GAVITT et al., 2011)** : Esta proposta é uma combinação da técnica de introspecção em máquina virtual e a integração com a API do hypervisor. O principal objetivo é diminuir o gap semântico para facilitar a análise da evidência. Para isso o autor implementa um API para transformar dados de baixo nível em informação de alto nível. Depende de cooperação do provedor de serviço de nuvem, não tem conhecimento da máquina hospedada e não vai além da coleta, não descreve como resolve a cadeia de custódia. Tem a vantagem de ser imune a técnicas anti-forenses. Quando comparado a este trabalho, a presente proposta tem por vantagens ser arcabouço de coleta e armazenamento de evidências não apenas um método de coleta. Empregando a estratégia de realizar a coleta diretamente na máquina não tem o problema do gap semântico próprio das soluções baseadas em introspecção. Como conhece o contexto do que está rodando dentro da máquina virtual podemos direcionar a coleta de modo que seja mais eficiente além do que a evidência coletada já é útil para análise.

- **Digital Forensics as a Service: A game changer (BAAR; BEEK; EIJK, 2014)** : Esta proposta é focada em uma mudança no armazenamento e forma de trabalho dos peritos forenses. Propõe que a forense seja oferecida como um serviço e que as evidências sejam armazenadas em um local centralizado com o devido controle de acesso e garantia de integridade da evidência. Descreve a arquitetura de armazenamento, qual o perfil que deve ter acesso a evidência e como é este acesso. Esta proposta não é focada apenas em incidentes na nuvem mas em qualquer outro incidente.

Embora seja uma ótima proposta de armazenamento de evidências e controle de acesso a elas, ele não descreve o processo de coleta nem de transporte. É uma proposta

focada mais na solução de problemas relacionados a manipulação da informação após a coleta, transporte e armazenamento. Não toca no assunto de coleta qualquer que seja, em nuvem ou física.

- **Live Digital Forensics in a Virtual Machine (ZHANG; ZHANG; WANG, 2010)** : Proposta para coletar informações de memória de máquinas virtuais através de instantâneos das mesmas. O metodo de coleta envolve tomar o instantâneo da máquina, no diretório onde o mesmo foi armazenado pegar o arquivo referente a memória e abri-lo / analisá-lo usando um programa de leitura de memória de mercado. O autor não trás detalhes do transporte, armazenamento ou controle de acesso. Precisa que a máquina exista para conseguir coletar a informação e o processo é dependente de intervenção humana. Analisando com mais cuidado é possível repetir a coleta mesmo sem a máquina existir uma vez que temos o instantâneo mas o autor não dá detalhes do caso.

Quando comparado a este trabalho, a presente proposta tem por vantagens a menor quantidade de informação necessária à investigação através da implementação da janela de x dias antes do incidente. Como o processo é automático, uma vez disparado não requer intervenção humana. A presente proposta descreve como garante a cadeia de custódia da evidência e consegue reproduzir o processo de coleta mesmo se a máquina não existir mais pois a evidência está atrelada ao container.

- **Comparative Analysis of volatile memory forensics (ALJAEDI et al., 2011)** : Levantamento sobre o impacto da realização de forense de memória ao vivo nas máquinas virtuais na nuvem. Mostra que a quantidade de informações referentes a processos não alocados e página de memória perdida é um ponto a considerar quando se inicia uma ferramenta para análise de memória em uma máquina já funcionando.

Quando comparado a este trabalho a presente proposta tem por vantagem estar sempre rodando na máquina virtual, sujeitando-se aos efeitos de escalonamento do processo e swap e assim não provoca as perdas de informações de processos não alocados e páginas de memória referentes ao rearranjo que o kernel faz quando uma nova aplicação é iniciada.

»» Colocar isso aqui em uma tabela ««

Solução: Automated forensic data acquisition in the cloud -> tempo para gerar o snapshot da instância de uma VM de 20 GB de tamanho x tamanho da memória alocada na VM:

512Mb -> 15 Seg  
1Gb -> 20 Seg  
4Gb -> 36 Seg

»» comparar com a quantidade de memória que eu salvo para viabilizar análise ««

Solução: Virtuoso, narrowing the semantic gap in virtual machine introspection -> comparativo do tamanho da evidência após a coleta, após a primeira filtragem e após a segunda x S.O.

Windows -> varios programas -> original [302082] -> primeira filtragem [230366]  
-> final [75141]  
Linux -> varios programas -> original [6107214]-> primeira filtragem [2265667]-> final [1095963]  
Haiku -> varios programas -> original [850363] -> primeira filtragem [702277] -> final [423438]

»» como métrica pensar em colocar isso focado em diminuição da quantidade de dados a serem analisados ««

Solução: Virtuoso, narrowing the semantic gap in virtual machine introspection -> análise da confiabilidade da evidência após o processos de filtragem x tamanho original da mesma

2 traces (???) -> 67% de confiança  
12 traces(???) -> 85% de confiança

Solução: Virtuoso, narrowing the semantic gap in virtual machine introspection -> Tempo para coleta dos dados para cada um dos programas utilizados como caso de investigação.

Windows -> varios programas -> tempo [751.9]  
Linux -> varios programas -> tempo [20723.9]  
Haiku -> varios programas -> tempo [1901.0]

»» vários programas utilizados para mensurar tempo, pegar uma media? «« »»  
comparar com o tempo que levo para gerar evidências ««

Solução: Comparative analisys of live memory forensics -> Quantidade média de processos que permaneceram na memória antes e depois de carregar a ferramenta x tamanho da memória alocada em uam VM

1Gb -> antes [78,33%] -> depois [61,66%]  
512Mb -> antes[73,33%] -> depois [46,66%]  
256Mg -> antes [50,55%] -> depois [35,00%]

»» comparar com a quantidade de memória alterada no meu caso ««

Solução: Comparative analisys of live memory forensics -> Quantidade média de página de memória alterada nos métodos de live analisys x memory imaging x tamanho da memória alocada em uam VM

,Gb -> live [7,99%] -> imaging [5,95]  
512Mb -> live[32,53%] -> imaging [8,75]  
256Mg -> live [52,37%] -> imaging [25,46]

»» Compara com a quantidade de memória alterada no meu caso ««

## 6 Análise dos Resultados

Aqui a análise dos resultados

# Referências

- ALJAEDI, A. et al. Comparative Analysis of Volatile Memory Forensics. *IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT) and IEEE International Conference on Social Computing (SocialCom)*, p. 1253–1258, 2011. Citado na página 11.
- BAAR, R. B. van; BEEK, H. M. A. van; EIJK, E. J. van. Digital Forensics as a Service: A game changer. *Digital Investigation*, Elsevier Ltd, v. 11, p. S54–S62, 2014. ISSN 17422876. Disponível em: <<http://dx.doi.org/10.1016/j.diin.2014.03.007>>. Citado na página 10.
- DEZFOULI, F. N. et al. Volatile memory acquisition using backup for forensic investigation. *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, p. 186–189, 2012. Citado na página 10.
- DOLAN-GAVITT, B. et al. Virtuoso: Narrowing the semantic gap in virtual machine introspection. *Proceedings - IEEE Symposium on Security and Privacy*, p. 297–312, 2011. ISSN 10816011. Citado na página 10.
- DYKSTRA, J.; SHERMAN, A. T. Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. *Digital Investigation*, Elsevier Ltd, v. 10, n. SUPPL., p. S87–S95, 2013. ISSN 17422876. Disponível em: <<http://dx.doi.org/10.1016/j.diin.2013.06.010>>. Citado na página 8.
- GEORGE, S.; VENTER, H.; THOMAS, F. Digital Forensic Framework for a Cloud Environment. p. 1–8, 2012. Citado na página 7.
- POISEL, R.; MALZER, E.; TJOA, S. Evidence and cloud computing: The virtual machine introspection approach. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, v. 4, n. 1, p. 135–152, 2013. ISSN 20935374 (ISSN). Disponível em: <<http://www.scopus.com/inward/record.url?eid=2-s2.0-84885399460{%&}partnerID=40{%&}md5=0e332690d4cb1f01934b540b53>>. Citado na página 7.
- REICHERT, Z.; RICHARDS, K.; YOSHIGOE, K. Automated forensic data acquisition in the cloud. *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, p. 725–730, 2015. Citado na página 9.
- SANG, T. A log-based approach to make digital forensics easier on cloud computing. *Proceedings of the 2013 3rd International Conference on Intelligent System Design and Engineering Applications, ISDEA 2013*, p. 91–94, 2013. Citado na página 9.
- ZHANG, L.; ZHANG, D.; WANG, L. Live Digital Forensics in a Virtual Machine. In: *2010 International Conference on Computer Application and System Modelling (ICCASM 2010)*. [S.l.: s.n.], 2010. v. 6, p. 328–332. Citado na página 11.