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 Metodolodia de Pesquisa Científica em Engenharia de Computação.

Universidade de São Paulo – USP

Escola Politécnica - Engenharia de Computação

Programa de Pós-Graduação em Engenharia Elétrica

São Paulo, Brasil

2016, v-0.1

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

Fig.	Area of the i^{th} component
456	Isto é um número
123	Isto é outro número
lauro cesar	este é o meu nome

Lista de símbolos

Γ	Letra grega Gama
Λ	Lambda
ζ	Letra grega minúscula zeta
$\in$	Pertence

Sumário

1 Introdução

Os crescentes avanços tecnilógicos que têm ajudado a vida do ser humano também trouxeram diversos novos tipos de crimes relacionados a tecnologia da informação. Segundo levantamento de 2015 do Colégio Notarial Brasileiro houve um aumento de 87% no número de atas que comprovam abusos e crimes virtuais (citação). Quando do evento de um crime, há a necessidade de preservar as evidências de modo que apoiem processos investigativos e legais mas também para que possamos compreender a sequência de eventos envolvidos no ataque de modo que possamos evitar que estas vulnerabilidades sejam exploradas novamente.

Ciência forense digital é uma ferramenta importante para a solução de crimes cometidos com um computador pela sua capacidade de reconstruir a cena do crime a partir das evidências digitais deixadas por um ataque. Com o crescente uso de ferramentas online, virtualização e hospedagem em nuvem, o volume de dados gerado por esses sistemas que já era uma preocupação da comunidade forense em 2008 (citação), hoje começou a inviabilizar algumas de suas práticas. (citação)

Coma funcionalidade da elasticidade de carga ofertada pelos provedores de nuvem, por meio da qual infraestrutura pode ser alocada e desalocada dinamicamente, veio à tona o problema da volatilidade dos dados nas máquinas virtuais. Com algumas ameaças que não deixam evidências em disco(citação), a memória de uma máquina despejada de um pool seria para sempre perdida. Com a máquina mais poderosa hoje ofertada pela Amazon tendo 240Gb de memória (citação), o ferramental forense disponível hoje esta pouco adaptado a desafios trazidos pela núvem (citação).

2 Justificativa

Falar das dificuldades para se realizar forense em sistemas em nuvem, do crescimentos dos crimes digitais, todos os crimes tem alguma parcela de evidência digital, da adoção da nuvem mundo a fora, da dificuldade das problemas de jurisdicao por causa da de implementação da nuvem do aspecto multi inquilino das implementacoes em nuvem. As características específicas da memória para este casos associadas ao caráter elástico das soluções em nuvem. Das tentativas em outros campos de tentar resolver essas questões técnicas. A necessidade de se submeter a regras de cunho legal para as provas geradas pela forense.

3 Objetivos

Declarar e explicar as 3 hipõteses do trabalho, associa-los ao objetivo principal e os 3 sub-objetivos

4 Plano de Trabalho

Não faço ideia de como faremos isso mas estou muito interessado em saber... :)

5 Material e Métodos

Implementação de virtualização de mercado. rede laboratorio

6 Análise dos Resultados

Nao faço a mais remota ideia de como fazer isso

7 Considerações finais

considerei finalmente que estamos gastando mais tempo formatando o documento do que realmente escrevendo seu conteúdo.

Referências